PLI PRACTISING LAW INSTITUTE

Intellectual Property
Course Handbook Series

Twentieth Annual Institute on Privacy and Data Security Law

Co-Chairs
Francoise Gilbert
Lisa J. Sotto
Thomas J. Smedinghoff

INTELLECTUAL PROPERTY
Course Handbook Series
Number G-1413

Twentieth Annual Institute on Privacy and Data Security Law

Co-Chairs
Francoise Gilbert
Lisa J. Sotto
Thomas J. Smedinghoff

To order this book, call (800) 260-4PLI or fax us at (800) 321-0093. Ask our Customer Service Department for PLI Item Number 251422, Dept. BAV5.

Practising Law Institute
1177 Avenue of the Americas
New York, New York 10036

 978-1-4024-3404-4

PLI Course Handbook Usage Policy

The Practising Law Institute publishes over 200 Course Handbooks each year. The primary function of each Course Handbook is to serve as an educational supplement for each program and to provide practical and useful information on the subject matter covered to attorneys and related professionals.

The printed and/or electronic copy of the Course Handbook each attendee and faculty member receives is intended for his or her individual use only. It is provided with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a professional should be sought. Please note the views and opinions published in this Course Handbook do not necessarily represent those of PLI.

Distribution of the Course Handbook or individual chapters is strictly prohibited, and receipt of the Course Handbook or individual chapters does not confer upon the recipient(s) any rights to reproduce, distribute, exhibit, or post the content without the express permission of the authors or copyright holders. This includes electronic distribution and downloading of materials to an internal or external server or to a shared drive. If a firm or organization would like to arrange access for a wider audience, printed copies of the Course Handbook are available at http://www.pli.edu. In addition, PLI offers firm or company-wide licensing of our publications through our eBook library, PLI Plus. For more information, visit https://plus.pli.edu.

The methods of reproduction, both print and electronic, were chosen to ensure that program registrants receive these materials as quickly as possible and in the most usable and practical form. The Practising Law Institute wishes to extend its appreciation to the authors and faculty for their contributions. These individuals exemplify the finest tradition of our profession by sharing their expertise with the legal community and allied professionals.

Prepared for distribution at the
TWENTIETH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY LAW
San Francisco, May 6–7, 2019
New York City, May 20–21, 2019
Chicago, June 3–4, 2019

CONTENTS:

PROGRAM SCHEDULE 13

FACULTY BIOS 35

1. California Consumer Privacy Act of 2018—Summary 125
   Francoise Gilbert
   Greenberg Traurig, LLP

2. Lisa J. Sotto, Aaron P. Simpson and Brittany Bacon, Hunton Andrews Kurth LLP, 2018 Retail Industry Year in Review: California Consumer Privacy Act and Its Impact on Retailers 179
   Submitted by:
   Lisa J. Sotto
   Aaron P. Simpson
   Hunton Andrews Kurth LLP

3. EU General Data Protection Regulation 185
   Francoise Gilbert
   Greenberg Traurig, LLP

4. GDPR: One Year Later (January 21, 2019) 283
   Ericka Watson
   Danaher Corporation

5. Miriam Wugmeister, Christine E. Lyon and Cynthia Rich, Privacy Laws Around the World (May 2019) 321
   Submitted by:
   Miriam Wugmeister
   Christine E. Lyon
   Morrison & Foerster LLP

6. An Overview of Cybersecurity Legal Requirements for All Businesses: 2019 Update 433
Thomas J. Smedinghoff
Locke Lord LLP

7. John Buchanan and Dustin Cho, Covington & Burling LLP, Ch. 17, Internet of Things (IoT): Legal, Policy, and Practical Strategies—When Things Get Hacked: Insurance Coverage for IoT-Related Risks (March 27, 2019) 495
Submitted by:
Marty Myers
Covington & Burling LLP

8. Hunton Andrews Kurth Client Alert, SEC Publishes New Guidance on Public Company Cybersecurity Disclosure (February 2018) 517
Submitted by:
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

9. A How-To Guide to Information Security Breaches, BNA, Inc., Privacy & Security Law Report, Vol. 6, No. 14, pp. 559–562 (April 2, 2007) 527
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

10. Aaron P. Simpson and Adam H. Solomon, Dealmakers Ignore Cyber Risks at Their Own Peril, Pratt's Privacy & Security Law Report, Vol. 1, No. 2, pp. 46–52 (October 2015) 535
Submitted by:
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

11. Jody Westby, *Cyber Crime Wave: Cyber Insurance Premium Growth Follows the Growing Wave of Cyber Crime*, Leader's Edge Magazine, May 2017 549

12. Jody Westby, *Inside Job: Consider the Range of Attacks Committed by Employees or Trusted Insiders*, Leader's Edge Magazine, June 2017 557

13. Jody Westby, *Starving Your IT Budget: Your Failure to Upgrade Means Your Luck May Be Over*, Leader's Edge Magazine, July/August 2017 565

14. Jody Westby, *Spreading Cyber Around: Cyber Coverage Is Popping Up in Multiple Places. Look Widely to Recover Claims*, Leader's Edge Magazine, October 2017 573

15. Jody Westby, *Cybering Up for Your Safety: This 15-Step Program Will Help You Recover from Unsafe Practices*, Leader's Edge Magazine, March 2018 581

16. Jody Westby, *Cyber Property: How Much Risk Do You Want to Keep In-House?*, Leader's Edge Magazine, October 2018 591

17. Jody Westby, *Preparing for New Cyber Threats: What's on the Horizon in 2019? Make Sure You've Got a Comprehensive and Tested Plan*, Leader's Edge Magazine, December 2018 599

18. The Latest Insights from Privacy and Data Security Regulators (June 3, 2019) 607

Attachment A: Table of Contents 609
Ruth Hill Bro
Privacy and cybersecurity attorney

Attachment B: Get SMART on Data Protection Training and How to Create a Culture of Awareness, Chapter 13, The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, ABA Cybersecurity Legal Task Force (2d ed. 2018), ambar.org/cybersecurity 613
Ruth Hill Bro
Privacy and cybersecurity attorney
Jill D. Rhodes
OptionCare Enterprises, Inc.

Attachment C: Lawyers' Legal Obligations to Provide Data Security, Chapter 4, The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals (ABA, 2018) 629
Ruth Hill Bro
Privacy and cybersecurity attorney
Thomas J. Smedinghoff
Locke Lord LLP

19. New York Attorney General, Press Release: A.G. Schneiderman Announces $575,000 Settlement With EmblemHealth After Data Breach Exposed Over 80,000 Social Security Numbers (March 6, 2018) 667
Submitted by:
Clark Russell
New York State Office of the Attorney General

20. New York Attorney General, Press Release: A.G. Underwood Announces Record $148 Million Settlement With Uber Over 2016 Data Breach (September 26, 2018) 673
Submitted by:
Clark Russell
New York State Office of the Attorney General

21. New York Attorney General, Press Release: A.G Underwood Announces Record COPPA Settlement With Oath – Formerly AOL – For Violating Children's Privacy (December 4, 2018) 681
Submitted by:
Clark Russell
New York State Office of the Attorney General

22. New York Attorney General, Press Release: A.G Underwood Announces Settlements with Five Companies Whose Mobile Apps Failed to Secure User Information Transmitted Over the Internet (December 14, 2018) 691
Submitted by:
Clark Russell
New York State Office of the Attorney General

23. Discoverability of Witness Interviews in California: Application of the Work Product Doctrine and the Attorney-Client Privilege 699
Merri A. Baldwin
Rogers Joseph O'Donnell

24. Steven E. Fagell, Benjamin S. Haley and Anthony Vitarelli, Covington & Burling LLP, Practical Guide for Maintaining Privilege Over an Internal Investigation (April 14, 2014) 707
Submitted by:
Merri A. Baldwin
Rogers Joseph O'Donnell
Kathryn J. Fritz
Fenwick & West LLP

25. The State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2012-183 731
Submitted by:
Merri A. Baldwin
Rogers Joseph O'Donnell
Kathryn J. Fritz
Fenwick & West LLP

26. Privacy and Security Developments in the Workplace (March 4, 2019) 739
Joseph J. Lazzarotti
Jackson Lewis P.C.
Rachel Roy
Sensata Technologies

27. Alan Charles Raul and Stephen W. McInerney, Litigation Risks: How to Mitigate Litigation Risks Associated with Data Security and Cyber Defense (March 5, 2019) 761
Submitted by:
Alan Charles Raul
Sidley Austin LLP

28. Tips from the Trenches to Make Your Company Less Attractive to Cyber Enforcement 779
Aimee Nolan
W.W. Grainger, Inc.
Jason N. Smolanoff
Kroll, a division of Duff & Phelps
Antony Kim
Orrick Herrington & Sutcliffe LLP

29. Considerations for Data-Rich Contracting Post-GDPR 801
Flora J. Garcia
McAfee, LLC

30. Managing Vendor Risks in a Changing Regulatory Landscape (March 11, 2019) 819
Maureen A. Young
Bank of the West

31. Mayer Brown Cybersecurity and Data Privacy Update 863
Submitted by:
Rebecca Eisner
Mayer Brown LLP

32. Hunton Andrews Kurth Client Alert: Privacy and Data Security Due Diligence in M&A Transactions (May 2017) 933
Submitted by:
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

33. Legal and Business Issues in AI, Big Data and IoT—A Practical Checklist 939
Lisa R. Lifshitz
Torkin Manes LLP

34. Privacy and Security Challenges of Advanced Technologies: Artificial Intelligence, Internet of Things, Big Data, and Blockchain 955
Stephen S. Wu
Silicon Valley Law Group

35. Blockchain: Challenges and Solutions for Compliance with the GDPR 985
Lydia de la Torre
Santa Clara Law School

36. Wiley Rein Newsletter: Moving Toward a New Health Care Privacy Paradigm (November 2014) 1005
Kirk J. Nahra
WilmerHale LLP (formerly with Wiley Rein LLP)

37. Wiley Rein Newsletter: Big Data, Privacy, Research, and De-Identification (December 2015) 1013
Kirk J. Nahra
WilmerHale LLP (formerly with Wiley Rein LLP)

38. Kirk J. Nahra and Bethany A. Corbin, Digital Health Regulatory Gaps in the United States, Compliance Elliance Journal, Vol. 4, No. 2, pp. 21–34 (2018) 1021
Submitted by:
Kirk J. Nahra
WilmerHale LLP

39. Bloomberg Law, Insight: The Top Five Health Care Privacy and Security Issues to Watch in 2019, BNA, Inc. (December 21, 2018) 1041
Kirk J. Nahra
WilmerHale LLP

40. Hunton Andrews Kurth LLP, Centre for Information Policy Leadership, Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice—First Report: Artificial Intelligence and Data Protection in Tension (October 10, 2018) 1047
Submitted by:
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

41. Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679 (October 4, 2017) 1073
Submitted by:
Lara Kehoe Hoffman
Netflix

42. Information Commissioner's Office: Sample DPIA Template 1103
Submitted by:
Lara Kehoe Hoffman
Netflix

43. Hunton Andrews Kurth LLP, Privacy & Information Security Law Blog: Global Privacy and Cybersecurity Law Updates and Analysis, European Data Protection Board Issues Privacy Shield Report (January 28, 2019) 1113
Submitted by:
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

INDEX 1129

Senior Program Attorney: Lauren E. Nochta

Program Schedule

Twentieth Annual Institute on Privacy and Data Security Law
San Francisco, May 6-7, 2019
New York City, May 20-21, 2019
Chicago, June 3-4, 2019

AGENDA DAY ONE

Morning Session:

9:00
Opening Remarks
SF & WEB: Francoise Gilbert
NY & WEB: Lisa J. Sotto
CHI: Francoise Gilbert, Thomas J. Smedinghoff

9:15
Complying with the California Consumer Privacy Act and other US Privacy Developments
- A detailed summary of the California Consumer Privacy Act of 2018
- Tips for compliance with the CCPA
- Leveraging your GDPR program for CCPA compliance
- The latest federal privacy proposals in the US
- Industry and expert proposals for a US privacy framework

SF & WEB: Francoise Gilbert, James G. Snell
NY & WEB: Kerry L. Childe, Adam J. Rivera, Lisa J. Sotto
CHI: Francoise Gilbert, James G. Snell

10:15
GDPR: One Year Later
- The latest interpretive guidance from the EDPB
- Clarifying extraterritorial reach: from offering goods and services to monitoring behavior
- Complying with data subject rights requests
- Status of available options for cross-border data transfers
- Enforcement trends: What are the priorities? How aggressive are they?
- Status of member state implementations

SF & WEB: Francoise Gilbert (Panel Leader), Darren Abernethy, Amanda Katzenstein, Emily Yu
NY & WEB: Alejandro Mosquera, Aaron P. Simpson
CHI: Jacob Springer, Ericka Watson

11:15 Networking Break

11:30

Beyond GDPR - Privacy and Data Security Compliance Around the World

- Privacy and security landscape outside the EEA
- Recent developments in Brazil and Latin America
- Recent developments in India and Asia
- How to manage the global cacophony of privacy and security laws

SF & WEB: Christine E. Lyon, Hilary M. Wandall
NY & WEB: Erika Brown Lee, Laura Juanes Micas, Miriam H. Wugmeister
CHI: Christine E. Lyon, Hilary M. Wandall

12:30 Lunch

Afternoon Session:

1:30

Cybersecurity Readiness: Addressing Compliance Risk

- What are the trends in US and foreign data security compliance requirements?
- Best practice approaches to developing a compliant security program
- What responsibilities do Boards of Directors have for data security and what is the latest case law?
- How can cyber insurance help in managing the risk?
- Dos and don'ts in making cyber-related insurance claims

SF & WEB: Marty Myers, Thomas J. Smedinghoff
NY & WEB: Deborah Hirschorn, Ryan Vinelli, David Wong
CHI: Marty Myers, Thomas J. Smedinghoff

2:30

Cybersecurity Attacks: A Survival Guide

- Incident response strategies
- Managing a forensic investigation
- Pros and cons of involving law enforcement
- Breach disclosure timing considerations
- Preparing for notification
- Managing the regulatory onslaught and inevitable lawsuits

SF & WEB: Michelle Visser, Jody Westby
NY & WEB: Eric M. Friedberg, Aristedes Mahairas, William E. Min
CHI: Steven R. Chabinsky, Jody Westby

3:30 Networking Break

3:45

The Latest Insights from Privacy and Data Security Regulators

- What gets the regulators' attention?
- What are the current regulatory priorities?
- How to best respond to an inquiry?
- How interested are the regulators in a company's security program?
- Enforcement coordination among regulators
- Biggest mistakes a company can make

SF & WEB: Dr. Jennifer King (Panel Leader), D. Esther Chavez, Jared Ho, Patrice Malloy, Stacey D. Schesser (invited)
NY & WEB: Michele S. Lucan, Maneesha Mithal, Clark Russell
CHI: Ruth Hill Bro (Panel Leader), D. Esther Chavez, Patrice Malloy, Maneesha Mithal, Matthew W. Van Hise

5:00 Adjourn

AGENDA DAY TWO

Morning Session:

9:00

Ethical Issues for Privacy and Data Security Professionals

- *Upjohn* and beyond: The attorney-client privilege and client confidentiality in connection with internal investigations
- Client misconduct: obligations and options for in-house and outside counsel
- Preparing for the worst: ethical obligations after a disaster; mistakes by lawyers; cybersecurity

SF & WEB: Merri A. Baldwin, Kathryn J. Fritz
NY & WEB: Alfred J. Saikali
CHI: Merri A. Baldwin, Kathryn J. Fritz

10:00

Internal Investigations – Balancing Employees Privacy Rights and Company's Goals and Obligations

- Structuring a Plan
- When and how to conduct an investigation
- He said / she said cases
- Maintaining confidentiality
- Unique issues with cross-border investigations

SF & WEB: Steven Cooper, John F. Hyland, Katherine L. Kettler
NY & WEB: Marianne Fogarty, Margaret A. Keane
CHI: Joseph J. Lazzarotti, Rachel Roy

11:00 Networking Break

11:15

Mitigating Litigation Risk: Lessons Learned from the Trenches

- Avoiding practices that may lead to trouble
- Managing a breach to avoid litigation
- Top claims plaintiffs are making
- Avoiding becoming a class action target
- Avoiding becoming an FTC, SEC or state AG target
- Settlement trends

SF & WEB: Jonathan D. Avila, Harvey Jang, Polina Zvyagina
NY & WEB: Stephanie Driggers, Alan Charles Raul
CHI: Antony Kim, Aimee Nolan, Jason N. Smolanoff

12:15 Lunch

1:15

Vendor Management: Ensuring Compliance with Privacy and Cybersecurity Requirements

- Scope of vendor management legal requirements
- Developing a compliant vendor management program
- Evaluating vendors from a privacy and security perspective
- Conducting due diligence of vendor privacy and security programs and practices
- Privacy and security provisions in vendor contracts
- Monitoring and auditing vendor compliance

SF & WEB: Flora J. Garcia, Maureen Young
NY & WEB: Kumneger Emiru, J. Andrew Heaton, Lesley Matty
CHI: Rebecca S. Eisner, Kathleen M. Porter

2:15

The Privacy and Security Challenges of New Technologies

- Addressing the privacy and security risks of using IoT devices
- Avoiding the snare of biometrics laws
- Deciphering the privacy and security issues raised by blockchain
- Privacy and data security issues in artificial intelligence

SF & WEB: Lydia de la Torre, Lisa R. Lifshitz, Stephen S. Wu
NY & WEB: Peter M. Lefkowitz, Kirk J. Nahra
CHI: Lisa R. Lifshitz, Stephen S. Wu

3:15 Networking Break

3:30

The Protectors: CPOs, CISOs and the Problem of Compliance Overload

- Twenty years in the making: how has the role evolved?
- What changes has the GDPR brought to the profession?
- What keeps them awake at night
- How to fight the “one size fits all” syndrome
- Communicating with regulators

SF & WEB: Lara Kehoe Hoffman (Panel Leader);
Jonathan D. Avila, Derek Care, Jonathan Fox, Alexandra Ross
NY & WEB: Keith Enright, Robert Lord, Zoe Strickland
CHI: Jonathan D. Avila, Andrew Sawyer

4:30 Adjourn

San Francisco Faculty:

Chair:

Francoise Gilbert
Greenberg Traurig, LLP
Silicon Valley, CA
Chair

Darren Abernethy
Senior Counsel
TrustArc
San Francisco

Jonathan D. Avila
Vice President, Chief Privacy Officer
Walmart Inc.
Bentonville, AR

Merri A. Baldwin
Rogers Joseph O'Donnell
San Francisco

Derek Care
Director II, Legal - Privacy
Uber Technologies, Inc.
San Francisco

D. Esther Chavez
Senior Assistant Attorney General, Consumer Protection Division
Office of the Texas Attorney General
Austin, TX

Steven Cooper
Associate General Counsel, Employment Law
Western Digital
Milpitas, CA

Lydia de la Torre
Privacy Fellow, Program Co-Director, Professor
Santa Clara Law School
Santa Clara, CA

Jonathan Fox
Director, Privacy Engineering, Strategy and Planning
Chief Privacy Office
Security & Trust Organization
Cisco
San Jose, CA

Kathryn J. Fritz
Fenwick & West LLP
San Francisco

Flora J. Garcia
Global Chief Privacy Officer
Privacy/Security Attorney
McAfee, LLC
Santa Clara, CA

Jared Ho
Senior Attorney
Division of Privacy & Identity Protection
Federal Trade Commission
San Francisco

Lara Kehoe Hoffman
Global Director of Data Privacy and Security, Legal
Netflix
Los Gatos, CA

John F. Hyland
Rukin Hyland & Riggin LLP
Oakland, CA

Harvey Jang
Senior Director, Global Data Protection & Privacy Counsel
Cisco Systems, Inc.
San Jose, CA

Amanda Katzenstein
Product and Privacy Counsel
Salesforce.org
San Francisco

Katherine L. Kettler
Director of U.S. Legal Investigations/Employment and
Labor Legal
Intel Corporation
Santa Clara, CA

Dr. Jennifer King
Director of Consumer Privacy, Center for Internet and Society
Stanford Law School
Stanford, CA

Lisa R. Lifshitz
Torkin Manes LLP
(Legal services provided through Lisa R.Lifshitz Professional
Corporation)
Toronto

Christine E. Lyon
Morrison & Foerster LLP
Palo Alto

Patrice Malloy
Chief, Multi-State and Privacy Bureau
Senior Assistant Attorney General
Office of the Attorney General
Fort Lauderdale, FL

Marty Myers
Covington & Burling LLP
San Francisco

Alexandra Ross
Director, Global Privacy and Data Security Counsel
Autodesk, Inc.
San Francisco

Stacey D. Schesser (invited)
Supervising Deputy Attorney General
Consumer Law Section - Privacy Unit
California Department of Justice
San Francisco

Thomas J. Smedinghoff
Locke Lord LLP
Chicago

James G. Snell
Perkins Coie LLP
Palo Alto

Michelle Visser
Orrick Herrington & Sutcliffe LLP
Boston and San Francisco

Hilary M. Wandall
Chief Data Governance Officer, General Counsel & Corporate Secretary
TrustArc
San Francisco

Jody Westby
Chief Executive Officer
Global Cyber Risk LLC
Washington, DC

Stephen S. Wu
Silicon Valley Law Group
San Jose

Maureen Young
Senior Regulatory Counsel, Senior Vice President
Bank of the West
San Francisco

Emily Yu
Senior Corporate Counsel
Global Privacy
Seagate Technology LLC
Cupertino, CA

Polina Zvyagina
Privacy Counsel
Airbnb
San Francisco

New York City Faculty:

Chair:

Lisa J. Sotto
Hunton Andrews Kurth LLP
New York City
Chair

Kerry L. Childe
(Former) Sr. Corporate Counsel, Privacy and Information Policy
Best Buy
Richfield, MN

Stephanie Driggers
Global Litigation Counsel
UPS
Atlanta

Kumneger Emiru
Senior Corporate Counsel
ServiceNow
Santa Clara, CA

Keith Enright
Chief Privacy Officer
Google LLC
Mountain View, CA

Marianne Fogarty
Senior Legal Director, Compliance
Twitter
San Francisco

Eric M. Friedberg
Co-President
Stroz Friedberg, an Aon company
New York City

J. Andrew Heaton
Global Lead Counsel - Data Privacy and Security
EY
Washington, DC

Deborah Hirschorn
Complex Claims Director
AIG
New York City

Margaret A. Keane
DLA Piper LLP (US)
San Francisco

Erika Brown Lee
Senior Vice President
Assistant General Counsel
Privacy and Data Protection
Mastercard
Purchase, NY

Peter M. Lefkowitz
Chief Privacy & Digital Risk Officer
Citrix Systems, Inc.
Burlington, MA

Robert Lord
Chief Security Officer
Democratic National Committee
Washington, DC

Michele S. Lucan
Assistant Attorney General
Privacy and Data Security Department
Office of the Attorney General
Hartford, CT

Aristedes Mahairas
Special Agent in Charge, Counterintelligence / Cyber Division
Federal Bureau of Investigation
New York City

Lesley Matty
Senior Counsel
Tiffany & Co.
New York City

Laura Juanes Micas
Global Director, Privacy Policy Engagement
Facebook
Miami

William E. Min
Deputy General Counsel & Chief Privacy and Data Governance Officer
The Western Union Company
Denver

Maneesha Mithal
Associate Director
Division of Privacy and Identity Protection
Federal Trade Commission
Washington, DC

Alejandro Mosquera
Director and Assistant General Counsel
MUFG
New York City

Kirk J. Nahra
WilmerHale
Washington, DC

Alan Charles Raul
Sidley Austin LLP
Washington, DC

Adam J. Rivera
Senior Counsel & Privacy Officer
Refinitiv
Stamford, CT

Clark Russell
Deputy Bureau Chief
Bureau of Internet and Technology
New York State Office of the Attorney General
New York City

Alfred J. Saikali
Shook, Hardy & Bacon L.L.P.
Miami

Aaron P. Simpson
Hunton Andrews Kurth LLP
London and New York City

Zoe Strickland
VP, Global Privacy and US Commercial Compliance
CIGNA
New York City

Ryan Vinelli
VP, Data Governance & Privacy Technology Counsel
Western Union
Montvale, NJ

David Wong
Vice President
Mandiant
New York City

Miriam H. Wugmeister
Morrison & Foerster LLP
New York City

Chicago Faculty List:

Co-Chairs:

Francoise Gilbert
Greenberg Traurig, LLP
Silicon Valley, CA
Co-Chair

Thomas J. Smedinghoff
Locke Lord LLP
Chicago
Co-Chair

Jonathan D. Avila
Vice President, Chief Privacy Officer
Walmart Inc.
Bentonville, AR

Merri A. Baldwin
Rogers Joseph O'Donnell
San Francisco

Ruth Hill Bro
Privacy and cybersecurity attorney
Chicago

Steven R. Chabinsky
White & Case LLP
Washington, DC

D. Esther Chavez
Senior Assistant Attorney General, Consumer Protection Division
Office of the Texas Attorney General
Austin, TX

Rebecca S. Eisner
Mayer Brown LLP
Chicago

Kathryn J. Fritz
Fenwick & West LLP
San Francisco

Antony Kim
Orrick Herrington & Sutcliffe LLP
Washington, DC

Joseph J. Lazzarotti
Jackson Lewis P.C.
Morristown, NJ

Lisa R. Lifshitz
Torkin Manes LLP
(Legal services provided through Lisa R.Lifshitz Professional Corporation)
Toronto

Christine E. Lyon
Morrison & Foerster LLP
Palo Alto

Patrice Malloy
Chief, Multi-State and Privacy Bureau
Senior Assistant Attorney General
Office of the Attorney General
Fort Lauderdale, FL

Maneesha Mithal
Associate Director
Division of Privacy and Identity Protection
Federal Trade Commission
Washington, DC

Marty Myers
Covington & Burling LLP
San Francisco

Aimee Nolan
Vice President, Associate General Counsel and Chief Intellectual Property Counsel
W.W. Grainger, Inc.
Lake Forest, IL

Kathleen M. Porter
Robinson & Cole LLP
Boston

Rachel Roy
Associate General Counsel, Global Employment and Compliance
Sensata Technologies
Attleboro, MA

Andrew Sawyer
Director of Security
Locke Lord LLP
Dallas

Jason N. Smolanoff
Senior Managing Director,
Global Practice Leader of Cyber Risk
Kroll, a division of Duff & Phelps
Los Angeles

James G. Snell
Perkins Coie LLP
Palo Alto

Jacob Springer
Division Counsel, Global Privacy Legal Lead
Abbott Laboratories
Abbott Park, IL

Matthew W. Van Hise
Assistant Attorney General
Chief, Privacy Unit
Consumer Fraud Bureau
Illinois Attorney General's Office
Springfield, IL

Hilary M. Wandall
Chief Data Governance Officer, General Counsel & Corporate Secretary
TrustArc
San Francisco

Ericka Watson
Lead Counsel
Global Data Privacy & EU Data Protection Officer
Danaher Corporation
Chicago

Jody Westby
Chief Executive Officer
Global Cyber Risk LLC
Washington, DC

Stephen S. Wu
Silicon Valley Law Group
San Jose

Senior Program Attorney: Lauren E. Nochta

Faculty Bios

Francoise Gilbert

Greenberg Traurig, LLP

PH: 650-804-1235; Email: gilbertf@gtlaw.com
SILICON VALLEY: 1900 University Avenue, 5th Floor, East Palo Alto, CA 94303
SAN FRANCISCO: 4 Embarcadero Center, Suite 3000, San Francisco, CA 94111

Francoise Gilbert focuses her practice on U.S. and global data privacy and cybersecurity in a wide variety of markets, including, among others, compliance with the European Union General Data Protection Regulation (GDPR) and other EU data protection laws, big data, cybersecurity, connected devices, intelligent vehicles, artificial intelligence, robots and other emerging technologies.

She counsels clients on complex issues related to evaluating and strategically managing privacy, security, and e-business risks. She assists in the design of product and services to help meet the company's objectives within the constraints of compliance requirements; the development of compliance programs to meet data protection laws in a variety of markets, including the EU, Asia/Pacific, Middle East / Africa, and the Americas. She also advises clients in the development of internal programs to help drive a culture of privacy across entire organizations; product development strategies aimed at meeting the privacy-by-design and security-by-design principles; and addressing privacy and security in mergers and acquisitions, and other corporate and commercial transactions.

A sought-after speaker, Francoise Gilbert has been featured on numerous panels throughout the United States and internationally on privacy, security, the EU General Data Protection Regulation (GDPR), global privacy programs, cloud computing, connected objects, smart cities, robot law, risk management, outsourcing, information technology, and e-business law by industry groups, bar associations and trade associations.

In addition, Ms. Gilbert is the author of the leading two-volume treatise "Global Privacy and Security Law" which covers in depth the privacy and data protection laws of 68 countries on all continents. She has written numerous chapters in collective works and has published hundreds of articles in peer-reviewed publications, professional journals and magazines on privacy, security, emerging technologies, compliance, cybercrime, outsourcing, workplace privacy, information law, data governance, Internet law, eCommerce, children protection, and comparative law.

Concentrations

- Information privacy and security, US and international

- Artificial intelligence
- Big data, data analytics
- Interest-based advertising
- Internet of Things, connected objects, intelligent vehicles, smart cities
- Complex technology licensing; cloud computing; outsourcing
- Blockchain

Lisa J. Sotto

Hunton Andrews Kurth LLP

LSotto@HuntonAK.com; 212.309.1223

Named among *The National Law Journal's* "100 Most Influential Lawyers," Lisa Sotto chairs Hunton Andrews Kurth's top-ranked Global Privacy and Cybersecurity practice and is the managing partner of the firm's New York office. She also serves on the firm's Executive Committee. Lisa has received widespread recognition for her work in the areas of privacy and cybersecurity. She was voted the world's leading privacy advisor in all surveys by *Computerworld* magazine and has received top rankings for privacy and data security by Chambers and Partners and The Legal 500. Lisa serves as the Chairperson of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Lisa assists clients in identifying, evaluating and managing risks associated with privacy and data security practices. She advises clients on GLB, HIPAA, COPPA, CAN-SPAM, FCRA, VPPA, security breach notification laws, and other U.S. state and federal privacy and data security requirements (including HR rules), and global data protection laws (including those in the EU, Asia and Latin America). More recently, Lisa's work includes assisting dozens of clients in developing strategies for complying with the California Consumer Privacy Act of 2018.

Featured as "The Queen of Breach" in an article by *New York Super Lawyers Magazine*, Lisa provides extensive advice on cybersecurity risks, incidents and policy issues, including proactive cyber incident readiness. Since 2005, she has advised clients on more than 1,600 cybersecurity and data breach incidents in the U.S. and abroad, including many of the seminal events. Lisa is the editor and lead author of the legal treatise entitled *Privacy and Cybersecurity Law Deskbook*, published by Aspen Publishers, Wolters Kluwer Law & Business.

Lisa is chair of the New York Privacy Officers' Forum and a former member of the Board of Directors of IAPP. She received her J.D. from the University of Pennsylvania Law School, where she was an editor of the Law Review. She received her B.A. from Cornell University, with Distinction in All Subjects. Lisa is admitted to practice in New York.

Thomas J. Smedinghoff
Locke Lord LLP
111 S. Wacker Drive, Chicago, Illinois 60606
PH: 312-201-2021; Email: Tom.Smedinghoff@lockelord.com

Thomas J. Smedinghoff is Of Counsel in the Privacy & Cybersecurity practice group in the Chicago office of Locke Lord LLP. His practice focuses on the developing field of information law and electronic business activities, and he has been actively involved in developing e-business, e-signature, identity management, and data security legal policy both in the U.S. and globally.

He currently serves as Co-Chair of the ABA's Cybersecurity Legal Task Force, and is Chair of the Identity Management Legal Task Force and Co-Chair of the Cybersecurity Subcommittee in the ABA Business Law Section. He is also an advisor to the U.S. Delegation to the United Nations Commission on International Trade Law (UNCITRAL), and in that capacity he helped to negotiate the international e-commerce treaty known as the *United Nations Convention on the Use of Electronic Communications in International Contracts.* He is currently working with UNCITRAL to address international electronic identity management issues. He also serves as an Advisor to the Uniform Law Commission Study Committee on Identity Management in Electronic Commerce.

Tom is co-editor and contributing author of the GUIDE TO CYBERSECURITY DUE DILIGENCE IN M&A TRANSACTIONS (ABA, 2017), and a contributing author to the 1st and 2nd editions of THE ABA CYBERSECURITY HANDBOOK - A RESOURCE FOR ATTORNEYS, LAW FIRMS & BUSINESS PROFESSIONALS (ABA, 2013 and 2018). He is also the author of the book titled INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE, (2008), and editor and primary author of the e-commerce book titled ONLINE LAW: THE LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET (1996). He can be reached at Tom.Smedinghoff@lockelord.com

Darren Abernethy

TrustArc Inc – Senior Counsel

darren@trustarc.com / (415) 766-6451

https://www.linkedin.com/in/djabernethy/

Darren Abernethy is Senior Counsel at the San Francisco headquarters of TrustArc Inc. Assisting customers for more than two decades, TrustArc is the global leader in privacy compliance technology solutions, privacy consulting and TRUSTe certification solutions, addressing all phases of companies' privacy program management and data governance.

At TrustArc, Darren provides product and legal advice for the company's portfolio of consent, advertising, marketing and consumer-facing technology solutions. He also helps manage the company's own privacy and data governance program; negotiates transactional and contractual matters; and interfaces with regulators, policy officials and TrustArc's industry partners and peers. Darren's areas of particular attention include EMEA data protection law, global digital advertising, the California Consumer Privacy Act, geolocation, cross-border data transfers and marketing regulations.

Prior to joining TrustArc, Darren practiced telecommunications law in private practice in Washington, D.C. In this capacity, he advised cable and broadband providers, cellular carriers, and members of the wireless spectrum ecosystem on FCC telecommunications matters and data privacy. After "going west" from Washington to San Francisco, Darren helped lead a marketing and management services agency focused on "smart," connected culinary devices prior to acquisition by its largest client.

A holder of the American Bar Association-IAPP Privacy Law Specialist designation and seven International Association of Privacy Professionals certifications, Darren is admitted to practice law in New York, Washington, D.C., and California.

When not privacy'ing, Darren attempts to play soccer for a recreational league team, enjoys hiking the S.F. Bay Area with family and friends, and welcomes a hearty pub quiz with colleagues. He also enjoys amateur astronomy and chipping away with his wife at their plan to visit and emboss their official U.S. National Park Passport with each of the 60 National Parks' stamps.

Jonathan D. Avila
Vice President and Chief Privacy Officer
Walmart Stores, Inc.

Jonathan Avila joined Walmart Stores, Inc. as Vice President, Chief Privacy Officer in October 2012. Mr. Avila is responsible for the worldwide data privacy and records management program for Walmart's operations involving 11,000 retail locations with more than two million employees in 27 countries, as well as Walmart's e-commerce websites in ten countries. Mr. Avila previously served as Vice President -- Counsel, Chief Privacy Officer of The Walt Disney Company. Mr. Avila initiated the data privacy program at Disney in 2001 and led the development of Disney's enterprise privacy compliance program covering all of Disney's online and offline business activities in the nearly 50 countries in which Disney operates.

Mr. Avila has been active in the international data privacy community, having served for five years on the board of directors of the International Association of Privacy Professionals, including serving as President of the IAPP in 2009. Mr. Avila has spoken at numerous conferences on data privacy issues, including conferences of the international data privacy commissioners sponsored by the governments of Spain and Mexico. Mr. Avila is a co-author of *Privacy Compliance and Litigation in California* (CEB 2014). Mr. Avila served on the advisory committee to the California Office of Privacy Protection on the development of its guidance on California's "Shine the Light" law relating to business' information sharing practices. Mr. Avila also has taught on the subject of privacy law as an Adjunct Professor of the School of Law of the University of Arkansas.

Mr. Avila began his career as a law clerk to Judge W. Eugene Davis of the United States Court of Appeals for the Fifth Circuit. Mr. Avila later was an associate with Latham & Watkins, and Litigation Counsel with the CBS television network. Before joining Disney, Mr. Avila served as General Counsel Chief Privacy Officer of MValue.com, Inc., a venture capital funded Internet company.

Mr. Avila graduated with a B.A. from Yale University and a J.D. from Harvard Law School. Mr. Avila also holds a diploma from the University of Salamanca (Spain) and holds the Certified Information Privacy Professional credential issued by the IAPP.

Merri A. Baldwin

Rogers Joseph O'donnell

Robert Dollar Building
311 California Street, 10th Fl., San Francisco, CA 94104
PH: 415-956-2828; Email: Mbaldwin@rjo.com

Merri Baldwin is a shareholder at Rogers Joseph O'Donnell in San Francisco, where her practice focuses on attorney liability and commercial litigation. She handles claims of legal malpractice and breach of fiduciary duty, as well as motions to disqualify and for sanctions. She regularly counsels lawyers and law firms on legal ethics and law practice management issues. She represents attorneys in disciplinary matters before the State Bar of California, and has extensive experience handling attorney-client fee disputes. Ms. Baldwin is a past chair of the State Bar of California Committee on Professional Responsibility and Conduct. She is a co-chair of the Legal Malpractice subcommittee for the American Bar Association Litigation Section Committee on Professional Services Litigation. Ms. Baldwin served as the President of the Bar Association of San Francisco for 2017. Ms. Baldwin frequently lectures to attorneys and professional organizations on issues related to litigation, legal malpractice and ethics issues, and she is a lecturer at the University of California at Berkeley School of Law, where she teaches professional responsibility. Ms. Baldwin co-edited The Law of Lawyers' Liability (ABA/First Chair Press 2012) and has served as a consulting editor for the Attorney Fee Agreement Forms Manual, published by Continuing Education of the Bar, California. Prior to law school, Ms. Baldwin was a Fulbright Scholar at the London School of Economics.

Education

J.D., University of California at Berkeley,
School of Law (Boalt Hall)

B.A., Smith College
Magna Cum Laude with high honors

Ruth Hill Bro

Privacy and Cybersecurity Attorney

PH: (630) 926-1273; Email: ruth.hill.bro@gmail.com

Ruth Hill Bro (Chicago) has focused her legal career on advising businesses on privacy and information management strategy, cybersecurity, global compliance, the electronic workplace, and e-business. She has been featured as a speaker on these issues over 160 times and has over 90 published works on these topics. These works include the first (2013) and second (2018) editions of *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals,* which won the 2018 ACLEA Best Publication Award (contributing author, ABA; ambar.org/cybersecurity); *Data Breach and Encryption Handbook* (two chapters, 2011, ABA); *The E-Business Legal Arsenal: Practitioner Agreements and Checklists* (Editor, 2004, ABA); *Internet in the Workplace: Managing Organizational Access* (designed and taught one-day course throughout the U.S. and co-authored book, 1997, Software Publishers Association); *Online Law* (five chapters, 1996, Addison-Wesley); and her column *CPO Corner: Interviews with Leading Chief Privacy Officers* (2005-present, published in *The SciTech Lawyer* magazine).

Ruth is a longstanding leader in the American Bar Association (ABA), where she co-chairs the ABA Cybersecurity Legal Task Force (ambar.org/cyber), serves on the ABA E-Mail Stakeholder Committee, and is a leader in the ABA Section of Science & Technology Law (SciTech). In SciTech, she is a Senior Advisor for the Privacy, Security, and Emerging Technology Division, a member of the Planning Committee (2015-2019) for the ABA's first four Internet of Things (IoT) National Institutes, and the Section's Liaison to the ABA Commission on Women in the Profession. She also served as SciTech's 2008-2009 Section Chair, Membership and Diversity Committee Chair (2009-2016), and E-Privacy Law Committee Founder and Chair (2000-2005). Ruth likewise served two three-year terms (2009-2015) on the ABA Standing Committee on Technology and Information Systems (the second term as Chair), as a liaison to the ABA Standing Committee on Continuing Legal Education (2012-2015), on the ABA Commission on the Future of Legal Services (2014-2016) (a two-year presidential commission to improve access to, and delivery of, legal services in the U.S.), on the ABA Standing Committee on Disaster Response and Preparedness (2016-2017), and on the ABA Board of Governors Communications Task Force (2017).

Ruth has served on many of the top advisory/editorial boards in the privacy, data security, and technology field (including *The SciTech Lawyer*, *DataGuidance* (U.S. Panel of Experts), *Internet Law & Strategy, The Privacy & Data Protection Legal Reporter* (Executive Editor/Chairman of the Board of Editors), and BNA's *Privacy &*

Security Law Report) in addition to the boards of two arts organizations and the Illinois Institute for Continuing Legal Education. She has been recognized as a leader by numerous organizations, including for four consecutive years in Ethisphere Institute's annual list of Attorneys Who Matter (data privacy/security). Her views have been noted by the *Wall Street Journal, International Herald Tribune, New York Times, Economist Intelligence Unit, ABA Journal, National Law Journal, Corporate Counsel, BNA Privacy & Security Law Report, CyberInsecurity News, FCW/Federal Computer Week, Legaltech News, Bloomberg Radio,* and *CNBC.*

Ruth started her legal career at McBride Baker & Coles (now Holland & Knight) and then spent nearly a decade at Baker & McKenzie, where she was a partner in the Chicago office and founding North American member of the firm's Global Privacy Steering Committee. Before getting her J.D. from the University of Chicago, Ruth had a successful career in major gifts fundraising at Northwestern University, where she earned her B.A. in English and Political Science. She won first place in *New York Law Journal's* fiction contest for her short story, *Privilege,* and before that second place in *Chicago Lawyer's* fiction contest for her short story, *Her Father's Daughter.*

Derek Care

Uber Technologies, Inc.

Derek Care is Director II, Privacy – Legal at Uber, a global transportation technology company headquartered in San Francisco, California. In this role, Derek is responsible for advising teams throughout Uber regarding global privacy requirements and best practices, including relating to the EU's General Data Protection Regulation and other global privacy laws. Derek is also responsible for implementing privacy policies, procedures and trainings; leading cross-company compliance efforts; and helping to embed privacy-by-design into Uber's operations. Prior to joining Uber, Derek was Privacy Counsel at Bloomberg LP, and before that, Counsel at Bingham McCutchen LLP.

Steven Chabinsky

White & Case LLP

PH: 202-626-3587; Email: steven.chabinsky@whitecase.com

Described as “One of the Most Influential People in Security,” Steven Chabinsky is the recipient of numerous awards and recognitions, including the National Intelligence Distinguished Service Medal, and serves as a trusted authority in cybersecurity.

Overview

Steve is a partner and the Chair of the Firm's Global Data, Privacy & Cybersecurity Practice. Steve advises domestic and international businesses on the wide range of data and network security compliance and risk management issues that enterprises face globally.

Clients benefit from Steve's extensive private sector and government experience focused on cybersecurity risks. His expertise includes cyber preparedness, incident response, information governance, data privacy, data breach regulatory response, government and internal investigations, reputation management, and the cybersecurity fiduciary duties of directors and officers.

A distinguished and trusted authority in the technology industry, Steve has dedicated nearly his entire career to cybersecurity. He has helped shape many of the nation's significant cyber and infrastructure protection strategies, including the Homeland Security Act of 2002 and the Comprehensive National Cybersecurity Initiative (2008). His impressive track record includes leading national intelligence efforts to coordinate, monitor and provide guidance with respect to America's national cyber strategy. In 2016, Steve was Presidentially appointed to the White House Commission on Enhancing National Cybersecurity. The Commission provided recommendations to the President to strengthen cybersecurity in the public and private sectors, while protecting privacy, fostering innovation and ensuring economic and national security.

Steve also is the cyber columnist for Security magazine.

Prior to joining White & Case, Steve served as General Counsel and Chief Risk Officer for an international cybersecurity technology firm, where he led the company's legal, privacy and risk programs and advised clients and their counsel on ways to protect their networks from being hacked and to respond effectively in the event of a data breach.

Before working in the private sector, Steve served as Deputy Assistant Director of the FBI's Cyber Division, after having organized and led its Cyber Intelligence program and

after having served as the FBI's top cyber lawyer. He also served as the senior cyber advisor to the United States Director of National Intelligence.

Prior to his work with the FBI, Steve held a clerkship with the Honorable Dennis Jacobs in the US Second Circuit Court of Appeals.

Bars and Courts
District of Columbia Bar
New York State Bar

Education
JD, Duke University School of Law
BA, Duke University

Languages
English

D. Esther Chavez

Office of the Texas Attorney General – Consumer Protection Division

D. ESTHER CHAVEZ currently serves as Senior Assistant Attorney General in the Consumer Protection Division of the Office of Texas Attorney General Ken Paxton where her work encompasses a broad range of consumer protection concerns with a focus on civil enforcement cases relating to privacy and data security.

Ms. Chavez' current professional activities include service as Chair of the Texas State Bar's Consumer & Commercial Law Council and as Course Director of the State Bar's 2018 Advanced Consumer & Commercial Law Conference.

Ms. Chavez is a frequent speaker at national and state continuing legal education seminars on a variety of privacy and consumer protection topics and most recently has been a presenter at the 22nd Annual Health Care Compliance Institute and the National Association of Attorneys' General Consumer Protection Spring and Fall 2018 Seminars.

Ms. Chavez obtained her undergraduate and legal education at the University of Texas at Austin and the University of Texas School of Law.

Kerry Childe

(Former) Senior Corporate Counsel for Privacy and Information Policy
Best Buy

Kerry Childe was the Senior Corporate Counsel for Privacy and Information Policy at Best Buy in Richfield, Minnesota, leading the Enterprise Privacy team as well as the Information and Records Management and Electronic Discovery teams. Prior to Best Buy, Kerry was the Senior Privacy and Regulatory Counsel for a nonprofit financial services company in Austin, Texas, focused on privacy matters, corporate governance, information technology, and business operations. Kerry received her JD from Baylor Law School in Waco, Texas, and her bachelor's degree from the University of Nebraska-Lincoln. She is currently on sabbatical, speaking at and attending conferences and working to discover her next adventure in privacy.

Steven M. Cooper

Western Digital Corporation
Associate General Counsel, Employment Law
Milpitas, CA

Steven M. Cooper is an Associate General Counsel, Employment Law, at Western Digital Corporation, where he has been since June 2014. He provides advice and counseling in all areas of employment law, including workplace investigations, wrongful termination litigation, performance management, compliance with anti-discrimination and leave laws, reasonable accommodations, mergers and acquisitions, and reductions in force. He has also trained managers and other employees on sexual harassment and other discrimination laws, managing within the law, and performance management.

Steven is also a member of the Western Digital Privacy team, focusing on the privacy rights of employees. In this role, he has been responsible for updating various policies, drafting privacy notices for employees, reviewing vendor agreements, providing advice on employee monitoring, and overseeing the records of processing activities program.

Before joining Western Digital, Steven served in both Legal and HR with Tesla Inc. and at DaVita Inc. Steven started his law practice at O'Melveny and Myers LLP in its Los Angeles office.

Steven earned his J.D., *magna cum laude*, from Hastings College of the Law, and his B.A., *cum laude*, from U.C. San Diego.

Lydia de la Torre
Santa Clara Law School

Lydia de la Torre joined Santa Clara in 2017 as the inaugural privacy fellow. She is the co-director of the Privacy Certificate program and teaches comparative data privacy. Her research centers on State data governance laws.

Lydia started working in data protection in 1997. She has extensive professional experience working on complex EU, US, and international data protection issues in the private sector. She started her career working as an Associate at Garrigues, a Spanish legal firm that provides business law advice in thirteen countries across Europe, Africa, Asia and the Americas. Professor de la Torre has worked as privacy counsel and consultant for fortune five hundred companies such as eBay, PayPal, Intuit and HP. Professor de la Torre's current areas of interest include EU data protection laws and data protection at the local and State level in California.

Lydia founded the legal blog 'Golden Data' (https://medium.com/golden-data) in 2018 with the goal of promoting the teaching of comparative privacy law. The blog includes teaching resources, case law analysis and op-eds on topics related to data governance laws including GDPR and CCPA.

Education
J.D., Univesidad Complutense Madrid (Spain)
L.L.M. EU Tax Law, Centro de Estudios Garrigues (Spain)
L.L.M. Intellectual Property, Santa Clara University School of Law

Areas of Specialization
Data Protection, Privacy, Cybersecurity

Affiliations and Honors
Member California Bar Association
Member Madrid Bar Association (Spain)
Member IAPP (CIPP/US Certified)
Member Internet Ethics Advisory Group – Markkula Center for Applied Ethics
Outstanding Faculty Award (2006 for teaching Legal Translation and Interpretation at the National Hispanic University)
2012/2013 LL.M. Student of the Year Santa Clara University School of Law

SAMPLE PUBLICATIONS

For IAPP:
“Is California on its way to going for ‘adequacy’?“ https://iapp.org/news/a/is-california-on-its-way-to-going-for-adequacy/
DPR matchup: The California Consumer Privacy Act 2018” https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/
“Do we need the CCPA whistle-blower provision back?” https://iapp.org/news/a/do-we-need-the-cacpa-whistleblower-provision-back/
SSRN
A guide to the California Consumer Privacy Act of 2108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275571
See also: https://medium.com/@dltsays_

Stephanie Driggers

United Parcel Service

(404) 828-4792

Stephanie Driggers is an Attorney with United Parcel Service, a global transportation and logistics company with operations in 220 countries and territories. She is responsible for managing complex commercial litigation both internationally and domestically across all business units. Ms. Driggers formerly had responsibility for global privacy, addressing tactical and strategic privacy and cybersecurity matters around the world.

Prior to joining UPS, Ms. Driggers was a partner at an Am Law 100 law firm, where she concentrated her practice on class action defense and data privacy litigation.

Ms. Driggers is a graduate of Vanderbilt University Law School and received her undergraduate degree from Stetson University. She clerked for Judge Thomas A. Wiseman, Jr. of the United Stated District Court in the Middle District of Tennessee. She is a Fellow of Information Privacy (FIP), a Certified Information Privacy Professional (CIPP-US), and a Certified Privacy Manager (CIPM).

Ms. Driggers focuses her pro bono and volunteer work on human trafficking.

Rebecca S. Eisner
Mayer Brown

Rebecca Eisner is a member of the Global Management Committee for the firm and previously served as a member of the Global Partnership Board and as Partner-in-Charge of the Chicago office. She has over 25 years of experience representing clients in hundreds of matters in three main areas: outsourcing, emerging technologies, and data privacy and security.

In outsourcing, Rebecca has represented clients in many industries in complex global technology and business process outsourcing transactions of all types. She also has experience with re-structuring and re-negotiating outsourcing transactions, in-sourcing, managing acquisitions and divestitures in outsourcing transactions, and termination of outsourcing arrangements, and other strategic sourcing relationships. In emerging technologies, Rebecca has advised clients negotiating with emerging technology providers on private and public cloud SaaS, PaaS and IaaS agreements and on appropriate regulatory, risk management, privacy, data protection, data use and analytics and licensing terms for cloud contracts. She has also represented clients in data acquisition and data analytics agreements. In traditional technology transactions, Rebecca has extensive experience in software development, robotic process automation and artificial intelligence agreements, database licensing and use agreements, ERP implementations, systems integrations, hosting and data center agreements and hardware acquisition and maintenance agreements. In security and data privacy, Rebecca regularly advises clients in global data transfers and privacy issues, privacy assessments, privacy compliance, and appropriate security and privacy measures in supply chain and third party contracting. She also advises on e-commerce issues, such as electronic contracting and signatures, and web site design and review. Rebecca is recognized as one of the leading lawyers in the outsourcing field by *Chambers Global* ("1" ranking in Outsourcing), *Chambers USA* ("1" ranking in "Nationwide: Outsourcing" and "Illinois: Technology & IT Outsourcing") and *Legal 500* (recognized in "Technology Outsourcing"). *Best Lawyers* named Rebecca as its Chicago Technology Lawyer of the Year for 2015. *Profiles in Diversity Journal* have named her a "Woman Worth Watching".

Kumneger Emiru

Senior Manager, Corporate Counsel, ServiceNow

Kumneger Emiru is a Senior Manager, Corporate Counsel at ServiceNow, where she focuses on global privacy compliance and manages ServiceNow's AMS privacy team. Kumneger serves as the lead negotiator on commercial transactions related to privacy for both inbound and outbound agreements. Her responsibilities also include product counseling and support and drafting privacy policies and procedures. During her tenure at ServiceNow, Kumneger also provided contract support to regional sales teams.

Kumneger previously worked at MongoDb supporting sales teams with commercial contracts, and at Workday, where her work included conducting privacy audits and trainings. She began her career at the Department of Health and Human Services, Office for Civil Rights, where she investigated alleged HIPAA violations.

Kumneger is a Certified Information Privacy Professional US/Europe. She received her law degree from the University of Iowa, College of Law and holds an A.B. from the University of Chicago with honors in dual concentrations of Public Policy and African and African American Studies.

Kumneger is admitted to practice in Illinois and is a registered in-house counsel in California.

Keith Enright
Google LLC

Keith Enright serves as Google's Chief Privacy Officer and leads the global privacy legal team. He joined Google in March 2011. He has nearly 20 years of experience in creating and implementing programs for privacy, data stewardship, and information risk management.

Prior to joining Google, Keith served as the senior-most privacy executive at two Fortune 500 online and offline retail enterprises, as senior consultant for a leading global consulting practice, and as General Counsel for a successful advertising technology company.

Keith served a 5-year term on the Board of Directors of the International Association of Privacy Professionals. He has been a guest speaker at Harvard Law School, Stanford Law School, and the Massachusetts Institute of Technology, and is frequently a featured speaker at industry events focusing on technology, privacy and data protection. He is a member of the Maryland Bar and holds the Certified Information Privacy Professional, U.S., and Government (CIPP/US, CIPP/G) certifications.

Marianne Fogarty

Senior Legal Director, Compliance

Twitter Inc.

Marianne Fogarty is the Senior Legal Director for Compliance at Twitter Inc. She is responsible for providing and executing the strategic vision for Twitter's Global Ethics and Compliance Program, leading efforts to identify and mitigate compliance risk and further embed the company's values. The Global Ethics and Compliance Program includes Ethics, Anti-Corruption, Trade Compliance and internal investigations of employee fraud and misconduct arising out of alleged violation of law and policy.

Prior to joining Twitter, Marianne was Senior Managing Counsel in MasterCard's Global Compliance group, and had responsibility for the development and day-to-day management of MasterCard's Code of Conduct and global ethics awareness and training, the global anti-corruption program and the regional compliance program. She also managed and conducted internal investigations of employee fraud and misconduct related to violations of the law, financial regulations and company policies.

Before going in-house, Marianne worked in private practice at Boies, Schiller & Flexner and Davis Polk & Wardwell on a variety of matters including, government and internal investigations, FCPA and anti-money laundering program development, complex commercial litigations and arbitrations, corporate criminal defense and representation of clients in a variety of legal and regulatory matters.

Ms. Fogarty is a graduate of Fordham Law School and the Wharton School of the University of Pennsylvania.

Jonathan Fox

Director, Privacy Engineering and Strategy and Planning
Chief Privacy Office
Cisco

Jonathan Fox, Director of Privacy Engineering and Strategy and Planning, is a member of Cisco's Chief Privacy Office and co-author of THE PRIVACY ENGINEER'S MANIFESTO, Getting from Policy to Code to QA to Value (ApressOpen 2014).

With over 17 years of privacy experience, Jonathan's principal areas of focus have been product development, government relations, mergers and acquisitions, and training. He is a Certified Information Privacy Professional (CIPP/US), a Certified Information Privacy Manager (CIPM), and was a Certified Information Security Manager (CISM).

Prior to Cisco, Jonathan was a Senior Privacy Engineer at Intel. His previous roles have included Director of Data Privacy, McAfee; Director of Privacy, eBay; Deputy Chief Privacy Officer for Sun Microsystems, and Editor-in-Chief of sun.com.

Jonathan frequently speaks at industry events and is a member of the IEEE P7002 Personal Data Privacy Working Group, the IAPP Privacy Engineering Section Forum Advisory Board, and the ISO/PC 317 Consumer Protection: Privacy by Design for Consumer Goods and Services US Technical Advisory Group.

Eric M. Friedberg

Co-President

Stroz Friedberg, an Aon company

Tel: 212-981-6536; Email: eric.friedberg@aon.com

Eric Friedberg is a seasoned executive with 30 years of public and private sector experience in law, cyber-crime response, IT security, forensics, investigations and e-discovery. His expertise is sought by boards, audit committees, law firms, and the courts. He has helped many Fortune 500 companies improve their governance and technology initiatives and their cyber regulatory compliance. He led Stroz Friedberg for over 16 years, from a start-up into a $150m, 550-person consulting and technical services firm with nine U.S. and four foreign offices. While always a principal business developer and leader of major client assignments, he oversaw geographic and service line growth, M&A, infusions of $150m in private equity capital, board interactions and, in late 2016, the sale of the company to Aon plc. Before the sale, Mr. Friedberg was an officer and director of Stroz Friedberg, and a member of the compensation committee.

Before building Stroz Friedberg, Mr. Friedberg was for 11 years a federal prosecutor in Brooklyn, where he led the Computer Crime and Narcotics Units. He began his career as an intellectual property and securities litigator at Skadden, Arps.

Mr. Friedberg is national leader in all forms of computer crime, including attacks by state-sponsored agents, organized crime, hacktivists, and malicious insiders. He has led responses to some of the most serious attacks on the nation's companies and has conducted enterprise security risk assessments in many sectors, including financial services, media and entertainment, Internet, sports, health care, law, consulting, oil and gas, and engineering. He is an expert in incident response governance, technologies, policies, and procedures. He has been quoted extensively on cyber-crime and IT security issues in print, digital and television media, including the Wall Street Journal, the Financial Times, The New York Times, cnbc.com, and Fox Business News.

Mr. Friedberg is also a leader in the fields of e-discovery, forensics and privacy, having managed hundreds of high-profile assignments in those areas, testified as an expert, been appointed by courts as a Special Master, and led the development of methodologies for forensic and privacy investigations. He has lectured extensively and has published book chapters and articles on managing risk and conducting investigations in e-discovery and forensics. He is a former member of the advisory board of the privacy think tank, The Future of Privacy Forum, and a member of the International Association of Privacy Professionals. He is a former member of the Sedona Conference's Working Group 6, which develops e-discovery standards.

At the U.S. Attorney's Office, Mr. Friedberg was a cybercrime, white collar crime, and narcotics prosecutor and worked extensively with the D.E.A., F.B.I., and U.S. Secret Service. He was also a member of the New York Electronic Crimes Task Force. His most prominent case was the investigation, prosecution and conviction of six accomplices who assassinated a former editor of the New York City Spanish daily newspaper El Diario on orders of the Cali Cartel in retaliation for unfavorable news coverage. For his leadership of the case, Mr. Friedberg received the 1994 Department of Justice Award for Superior Performance. In the cyber arena, Mr. Friedberg investigated and prosecuted cases involving hacking, denial of service attacks, propagation of malicious viruses, illegal data wiretapping, and cyber-extortion.

Mr. Friedberg holds a J.D. from Brooklyn Law School and a B.A. from Brandeis University.

Kathryn J. Fritz
Partner, Litigation, Intellectual Property and Privacy Groups
Fenwick & West LLP
PH: 415.875.2328**;** Email: kfritz@fenwick.com

Kathryn J. Fritz is a partner in the Litigation, Intellectual Property and Privacy Groups of Fenwick & West, a law firm focusing on technology and life sciences matters. Ms. Fritz is resident in the firm's San Francisco office. She served as the firm's Managing Partner from 2006 through 2017.

Ms. Fritz's practice concentrates on business and intellectual property litigation, with an emphasis on trademark, right of publicity and copyright, especially as applied to new technology areas. She has represented and advised software publishers, computer hardware manufacturers, gaming and digital media companies, entertainment companies, traditional media publishers and consumer products companies on commercial and intellectual property issues.

PROFESSIONAL ACTIVITES AND RECOGNITION
Ms. Fritz writes and speaks regularly on intellectual property issues to groups that include the Federal Judicial Center and Practicing Law Institute, and since 1999 has taught an advanced trademark law seminar at UC Berkeley School of Law.
She was named to The National Law Journal's 75 Outstanding Women Lawyers in 2015; has been named to The Recorder's list of Top 50 Women Leaders in Tech Law and, in 2015, was additionally designated as one of 10 "Power Players."
Ms. Fritz has been a member of the Board of Trustees of the Santa Clara County Bar Association and the Board of Directors of the Bar Association of San Francisco, and she is active in diversity initiatives in the profession.

PRO BONO INVOLEMENT
Ms. Fritz has been actively involved in pro bono, representing documentary filmmakers in intellectual property matters, a client on California's death row in this federal habeas corpus petition, ultimately achieving a reversal of his death sentence, and clients in political asylum petitions.

Ms. Fritz is also active in the greater pro bono community. She is currently a member of the Board of Directors of Equal Justice Works and the Board of Directors of Bay Area Legal Aid, and a member of the Pro Bono Institute's Law Firm Advisory Board. She previously served the Legal Service Corporation's Pro Bono Task Force and was co-chair of its Subcommittee on Technology Best Practices. She was recently honored by OneJustice for her pro bono leadership.

EDUCATION AND ADMISSIONS

Ms. Fritz received her B.A., magna cum laude, from the University of California at Santa Barbara, where she was a member of Phi Beta Kappa and a University of California Regents' Scholar. She received her J.D., cum laude, from Georgetown University Law Center, where she was Research Editor of the American Criminal Law Review. She is a member of the State Bars of New York and California, and numerous federal courts.

Flora J. Garcia
Global Chief Privacy Officer and Security Attorney
McAfee, LLC
Flora_Garcia@McAfee.com

Flora J. Garcia discovered privacy law one snowy night in law school when she read the case of Bodil Lindqvist, a Swedish woman who was the first person charged with violating the EU Privacy Directive. Flora is McAfee's Global Chief Privacy Officer and Security Attorney, after stints on other in-house teams and in information security and in compliance at MUFG Union Bank and magazine publisher Time Inc. She spearheaded McAfee's GDPR preparedness program.

Flora is a graduate of the evening program at Fordham Law School, the University of North Carolina at Chapel Hill's Journalism School, and Duke University, where she majored in computer science and economics. Flora is an IAPP Fellow of Information Privacy and holds the CIPP/US, CIPP/IT, and CISSP certifications.

J. Andrew Heaton

Global Lead Counsel – Data Privacy and Security

EY

J. Andrew Heaton is a principal in Ernst & Young LLP and serves as Global Lead Counsel – Data Privacy and Security for the global EY organization. In this role, he leads EY's global data protection team, serves as global privacy officer for the organization, and advises EY on legal aspects of data protection and information technology worldwide. Prior to assuming his global responsibilities in 2014, he served in a similar capacity with EY's practice in the United States, and was also lead counsel for EY's financial services practice.

Mr. Heaton graduated *summa cum laude* from Bradley University in Illinois. He received his law degree with honors from the University of Chicago Law School. He joined EY in 1994 and was named a principal in 2000.

Mr. Heaton is a Certified Information Privacy Manager, a Certified Information Privacy Professional/US, and a member of the bars of New York, the District of Columbia and Maryland.

Deborah Hirschorn
AIG

Deborah Hirschorn is an experienced Complex Director with a demonstrated history of working in the insurance industry. She is skilled in Professional Liability, Property & Casualty Insurance, Litigation Management, Arbitration, and Reinsurance. Deborah is a strong media and communication professional and graduated from Suffolk University Law School.

Jah-Juin "Jared" Ho

Senior Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
Washington, D.C.

Jah-Juin "Jared" Ho is an attorney with the Division of Privacy and Identity Protection (DPIP) at the Federal Trade Commission. This Division of the FTC has responsibility for enforcing federal statutes and regulations that pertain to information security and consumer privacy. Jared investigates and prosecutes violations of U.S. federal laws governing the privacy and security of consumer information and has worked on FTC enforcement actions under Section 5 of the Federal Trade Commission Act. Prior to joining DPIP, Jared was an attorney in the FTC's Office of Technology Research and Investigations. Jared has also served as a Senior Policy Advisor in the Federal Communications Commission's Enforcement Bureau where he advised on cases and rulemaking.

In addition to his federal service, Jared was a Deputy Attorney General for the State of New Jersey where he led his office's privacy and data security efforts. He has also served as a visiting fellow at Princeton University's Center for Information Technology Policy.

Lara Kehoe Hoffman

Netflix

Lara Kehoe Hoffman (CIPP/US, CIPP/E) is Chief Privacy Officer at Netflix, the world's leading internet entertainment service. Lara joined Netflix in January 2015, bringing with her a passion for building and improving data protection programs, and promoting a pro-privacy culture. Lara has domain expertise in GDPR, information management, education and kids privacy, among other areas. In her legal career Lara has represented a diverse array of clients from start-ups to multinationals in businesses ranging from technology to retail to children's toys.

Lara attended the University of San Diego, School of Law and has a degree in Comparative Literature from Yale.

John F. Hyland

Rukin Hyland & Riggin LLP

1939 Harrison Street, Suite 290, Oakland, California 94612
PH: 415.421.1800 (x202); Email: jhyland@rukinhyland.com

John F. Hyland has primarily focused his practice to employment law since his admission to the Bar in 1995. Prior to forming Rukin Hyland & Riggin LLP, John held an Of Counsel position with Paul Hastings, LLP in the firm's San Francisco office where he advised and represented companies in State and Federal court actions covering all areas of employment law, including wrongful termination, discrimination, harassment, disability law, employee privacy, employee leaves, and wage and hour issues. John has represented clients in jury trials and arbitrations, and he has argued cases before the California Court of Appeal. He continues to advise and represent clients in all areas of employment law and in commercial and business disputes.

John serves as an editor and contributing author for the CEB Publication, *Employee Leave Laws: Compliance and Litigation* (2016). John also serves as a contributing author to the Thompson Reuters *Inside the Minds* publications. John regularly conducts training seminars and presents on a wide array of employment law issues. He serves as an instructor for the Sonoma State University Human Resources Certification Program.

Law & Politics Magazine selected John as one of its Northern California Super Lawyers each year from 2006 through 2012, and again in 2014-18. *The Best Lawyers in America* has selected John for inclusion in each edition since 2012.

In addition to his litigation and counseling practice, John devotes a significant part of his practice to serving as a mediator. John obtained certification as an employment law mediator from Cornell University's School of Industrial Relations. He served as a mediator for the Sonoma County Superior Court ADR Program in which he mediated a wide array of civil cases, and he continues to serve as a panelist for the Court's settlement conference program. John is also a member of the Early Neutral Evaluation Program for the United States District Court for the Northern District of California for which he serves as an evaluator.

John received his B.S. degree from Saint Joseph's University in Philadelphia, Pennsylvania. He earned his J.D. degree from Golden Gate University School of Law in San Francisco, where graduated in 1995 with highest honors and first in his class. While at Golden Gate, John served as a contributing author and associate editor for the Golden Gate Law Review.

Harvey Jang

Senior Director, Global Data Protection & Privacy Counsel
APJC Data Protection & Privacy Officer
Cisco Systems, Inc.

Harvey Jang is Senior Director, Global Data Protection & Privacy Counsel and APJC Data Protection & Privacy Officer for Cisco. He serves as the team lead for privacy and data security related legal matters and is responsible for developing and orchestrating Cisco's global data protection policies, compliance capabilities, certifications, and accountability frameworks. Harvey also has primary responsibility for privacy strategy in Asia Pacific, Japan, and China (APJC) region for Cisco.

Prior to joining Cisco, Harvey was Senior Director, Legal Affairs for McAfee. Part of Intel Security where he was lead counsel for privacy, security, marketing, and antitrust compliance. In this role, he worked closely with engineers and product teams to develop and implement data protection policies and practices, design privacy enhancing products and functionality, and manage legal compliance. Before McAfee, Harvey was the Director of Privacy & Information Management and Chief Privacy & Security Counsel for HP; Senior Compliance Counsel for Symantec; and Litigation Counsel with O'Melveny & Myers LLP.

He is a member of the Board of Trustees for Bowman School in Palo Alto, serves as an instructor for the International Association of Privacy Professional's privacy credentials (CIPP/US, CIPP/Europe, and CIP/Technologist), and is a frequent panelists/speaker on a variety of topics related to privacy, security, and information governance.

Harvey earned his B.A., *magna cum* laude, from UCLA and his J.D., *cum laude*, from U.C. Hastings College of the Law. He is also a Fellow of Information Privacy (by IAPP), Certified Information Security Manager (by ISACA), and Certified Information Professional (by AIIM).

Amanda Katzenstein
Product and Privacy Counsel
Salesforce.org

Amanda Katzenstein is Product and Privacy Counsel at Salesforce.org, the philanthropic arm of Salesforce, which serves non-profits and educational institutions worldwide. In this role, she is responsible for deploying a global privacy program and provides day-to-day legal guidance to internal clients on privacy and data protection matters. She also spends significant time counseling product teams through all phases of product development, particularly in the education sector.

Before joining Salesforce.org, Amanda worked at multiple law firms, concentrating in intellectual property, litigation, and privacy law. These firms include Polsinelli PC, Novak Druce Connolly Bove + Quigg LLP, and Greenberg Traurig LLP.

Prior to becoming a lawyer, Amanda obtained extensive media and technology experience through industry positions. Her experience includes dealing with the practical effects of trademark rights at a national advertising agency, analyzing music licenses at a well-known music TV station, helping to build the legal department at an online media company, and assisting with media transactions at the Federal Communication Commission. She started her career in television, serving as a reporter and producer for news stations in Chicago and working in production for a nationally syndicated TV talk show.

Amanda holds the CIPP/US and CIPP/E credentials from the International Association of Privacy Professionals. She earned her law degree from Washington University in St. Louis and her undergraduate degree in journalism from Northwestern University. She is admitted to practice in California and New York.

Margaret Keane

DLA Piper LLP (US)

Margaret Keane is a Partner in the employment group at the international firm of DLA Piper LLP. She is based in San Francisco and works with clients to address the challenges of today's workplace, including workplace privacy, employee mobility issues, mobile devices, wage and hour compliance, and related workplace issues.

Katherine L. Kettler

Director of U.S. Legal Investigations/Employment, Labor & Benefits Legal
Intel Corporation

Katherine L. Kettler is the Director of US Legal Investigations/Employment Law. She leads a team of investigators who review internal claims of harassment, discrimination and retaliation. Katherine has been an employment law attorney for almost 20 years with a focus on employment litigation and counseling in all aspects of labor and employment law, including ADA and leave of absence compliance, discrimination avoidance, sexual harassment and diversity/inclusion programs.

Education
J.D. *summa cum laude* – Boston College Law School; Newton, MA
M.S.W. – University of Pennsylvania; Philadelphia, PA
B.A. -- Bar College; Annandale-on-Hudson, NY

Prior Law Firm Affiliations
Miller Law Group
Paul Hastings Janofsky & Walker
Ropes & Gray

Professional Recognition
Named a “Rising Star” by Super Lawyers – Northern California magazine in 2010 and 2011

Clerkship
Federal Court, District of Massachusetts

Bar Admissions
California

Antony (Tony) P. Kim

Partner – Cyber, Privacy & Data Innovation
Orrick, Herrington & Sutcliffe LLP
akim@orrick.com | (202) 339-8493

Antony (Tony) Kim is a partner in Orrick's global Cyber, Privacy & Data Innovation practice, which according to *The Legal 500* pursues "an aggressive yet practical approach" to data protection and innovation that "meets the needs of both in-house counsel and tech-savvy business clients."

When faced with a cyber crisis, companies call on Tony to help navigate critical legal and reputational landmines. Tony has helped clients respond to hundreds of cyberattacks and data breaches. He has directed forensic investigations, cross-border notifications, and defended enforcement actions and civil litigation, in connection with incidents involving the personal information of employees and customers, including PCI/payment card data, as well as trade secrets, on behalf of private and public companies as well as governmental entities.

Tony has also defended over fifty clients in regulatory investigations and enforcement actions by the Federal Trade Commission (FTC) and State Attorneys General. These matters have involved (i) cybersecurity and data breach incidents, (ii) privacy implications of innovative data use-cases, and (iii) consumer protection claims relating to online and offline sales & marketing and advertising practices – particularly in the retail e-commerce and fintech/consumer finance industries. Tony draws insights from his regulatory practice to inform his counseling work, where he regularly advises Legal, InfoSec/IT, Product/Marketing, and C-Suite/Board stakeholders on a host of governance, compliance, and risk mitigation strategies.

For his work on behalf of clients, Tony was named to the *National Law Journal's* 2014 list of D.C. Rising Stars, a 40-under-40 group of "game changing" private, government and public interest attorneys. Based on surveys of senior in-house lawyers, Tony was awarded the Client Choice Award by the *International Law Office (ILO)/Lexology* in 2015, and was named an *Acritas Star Lawyer* in 2016 and 2017. He is recognized in many other legal guides and directories, including *Chambers-U.S.A., The Legal 500-USA, Benchmark Litigation, Super Lawyers-D.C. Rising Stars,* and *The Cybersecurity Docket* -- which twice named Tony to its "Incident Response 30" list of the top professionals to call when facing a major cyberattack. In 2016, Law360 named Orrick's Cyber, Privacy & Data Innovation practice "Practice Group of the Year" in the data privacy category.

Tony earned his B.A. from Yale University, and a J.D. from the Georgetown University Law Center. Tony and his wife, Erin, have not slept since 2010 when the older of their two boys was born.

Jennifer King, Ph.D

Director of Consumer Privacy, Center for Internet and Society, Stanford Law School

jenking@law.stanford.edu

Dr. Jennifer King is the Director of Privacy at CIS. An information scientist by training, Dr. King is a recognized expert and scholar in information privacy. She examines the public's understanding and expectations of online privacy and the policy implications of emerging technologies. Her research sits at the intersection of human-computer interaction, law, and the social sciences, focusing on social media, genetic privacy, mobile platforms, the Internet of Things (IoT), and digital surveillance. Her scholarship has been recognized for its impact on policymaking by the Future of Privacy Forum, and she has been an invited speaker before the Federal Trade Commission at several Commission workshops. She was a member of the California State Advisory Board on Mobile Privacy Policies and the California State RFID Advisory Board.

Dr. King completed her doctorate in Information Science at the University of California, Berkeley School of Information. Her dissertation, "Privacy, Disclosure, and Social Exchange Theory," was named the runner up for the annual Information Schools (I-Schools) Organization Dissertation Award (2019). Prior to joining CIS, Dr. King was a co-director of the Center for Technology, Society, and Policy, a graduate student led research center at UC Berkeley, and was a privacy researcher at the Samuelson Law, Technology, and Public Policy Clinic at Berkeley Law. She received her Master's in Information Management and Systems also from the University of California, Berkeley's School of Information, and her undergraduate degree from the University of California, Irvine. Prior to entering academia she worked in security and in product management for several Internet companies, most notably Yahoo!.

Joseph J. Lazzarotti

Jackson Lewis P.C.

Joseph J. Lazzarotti is a Principal in the Morristown, New Jersey office of Jackson Lewis P.C. He founded and currently leads the Firm's Privacy, e-Communication and Data Security Practice, edits the Firm's Privacy Blog, and is a Certified Information Privacy Professional (CIPP) with the International Association of Privacy Professionals. He also is a leading member of the Firm's Health Care Reform Taskforce within our Employee Benefits Practice Group, and as a member of the Firm's Disability, Leave and Health Management Practice Group, he draws on his employee benefits and privacy experience to lead that group's Wellness Program Compliance Team.

In short, his practice focuses on the matrix of laws governing the privacy, security and management of data, as well as the impact and regulation of social media. He also counsels companies on compliance, fiduciary, taxation, and administrative matters with respect to employee benefit plans, and in particular with regard to group health plans under the Affordable Care Act, ERISA, HIPAA, ADA, GINA and other federal and state laws.

As a part of Joe's work in the area of privacy, e-communication and data security, he counsels multinational, national and regional companies in all industries on the broad array of mandates, best practices and preventive safeguards. For example, he advises health care providers and group health plan sponsors concerning HIPAA/HITECH compliance, as well as retail, health care, entertainment and other companies in developing data security and social media strategies and policies. He has worked on more than 500 data breach matters large and small, involving personal information concerning customers, patients, students, employees and others. His work includes conducting risk and vulnerability assessments, developing written information security programs (WISPs) and delivering on-site executive and employee trainings to help clients avoid breaches of personal information and achieve compliance. He has also represented companies with respect to inquiries and investigations concerning data privacy and security from the HHS Office of Civil Rights, Federal Trade Commission, State Attorneys General and other agencies, as well as in connection with negotiation of numerous business associate agreements and other data security agreements.

Joe's Employee Benefits Group work includes advising employers and plan sponsors regarding the establishment, administration and operation of retirement plans, as well as fully insured and self-funded group health and welfare plans, which includes counseling concerning the ACA. This includes helping clients setup administrative

arrangements with third-party administrators, claims administrators and other vendors. He has particular expertise on issues concerning design, compliance and implementation of wellness programs, including with regard to ACA and EEOC regulatory compliance. His work often involves day-to-day legal advice concerning employee benefit plan operation and administration and trouble-shooting with respect to errors in operation for retirement and welfare plans, including severance and fringe benefit plans.

Joe speaks and writes regularly on current employee benefits and data privacy and security topics and his work has been published in leading employment and business journals such as Bender's Labor and Employment Bulletin, the Australian Privacy Law Bulletin and the Privacy and Data Security Law Journal. His comments on these issues have been quoted in a number of media outlets, including Reuters, Inside Counsel, Politico, The National Law Journal, Employee Benefits News, Financial Times, Business Insurance Magazine, HR Magazine, and NPR.

Prior to joining Jackson Lewis, Joe was an employee benefits and privacy attorney with a large firm based in Kansas City, MO. He served as a judicial law clerk for the Honorable Laura Denvir Stith on the Missouri Court of Appeals. He holds a B.B.A. in public accounting, cum laude, from Pace University, and a J.D., with distinction, from the University Missouri-Kansas City School of Law.

Erika Brown Lee

Senior Vice President and Assistant General Counsel
Mastercard

Erika Brown Lee is a Senior Vice President and Assistant General Counsel at Mastercard. Ms. Brown Lee leads the team that develops policies, provides guidance, and ensures compliance with privacy and data protection laws across the company's products and services, including payment processing, data analytics, and fraud-related activities for North America, Latin America and the Caribbean. Ms. Brown Lee also works closely with the company's cybersecurity teams to develop policies and manage regulatory interactions. Ms. Brown Lee is the former Chief Privacy and Civil Liberties Officer of the U.S. Department of Justice, where she served as the principal advisor to the Attorney General on privacy and civil liberties matters. Ms. Brown Lee co-chaired the DOJ breach response team, played a leadership role among agencies working to develop privacy-related legislation, and provided regular briefings to Capitol Hill. She received an Attorney General Award for Exceptional Contributions in Negotiating a Data Protection and Privacy Agreement with the E.U. Ms. Brown Lee also served in the Division of Privacy & Identity Protection at the Federal Trade Commission, and chaired the ABA's Privacy & Information Security Committee. Ms. Brown Lee is a Certified Information Privacy Professional (CIPP) for Europe and the U.S.

Peter Lefkowitz

Chief Privacy & Digital Risk Officer, Citrix

Peter Lefkowitz is Chief Privacy & Digital Risk Officer at Citrix Systems. Peter oversees legal and regulatory risk associated with data, products and systems, as well as policy engagement on digital issues. Prior to joining Citrix, Peter worked at GE, where he served as Chief Privacy Officer (Corporate) and then as Senior Data Rights Management Counsel (Digital) and at Oracle, where he was Vice President of Privacy and Security Legal and Chief Privacy Officer. Peter is Chairman of the Board of the International Association of Privacy Professionals and a member of the Boston Bar Association Council. Peter holds a Bachelor of Arts in History, magna cum laude, from Yale College and a law degree from Harvard Law School.

Lisa R. Lifshitz

Torkin Manes LLP

Tel: 416 775 882 **Fax:** 1 877 689 389 **Email:** llifshitz@torkinmanes.com

Lisa Lifshitz is a partner in Torkin Manes' Business Law Group, specializing in the areas of information technology and business law and is the leader of the firm's Technology, Privacy & Data Management Group and Emerging Technology Group.

Lisa has particular expertise in preparing and negotiating technology agreements, including Internet-related, m-commerce and e-commerce agreements, cloud computing agreements, mobile payment agreements and outsourcing, system acquisition and master services agreements. She provides technology-related advice on financings and acquisitions, including export control/open source advice on cross-border deals. She also provides guidance on IoT, AI/smart contracts, blockchain and open source legal matters. Lisa has considerable experience helping non-Canadian companies, especially American entities, create appropriate legal agreements for their entry into the Canadian marketplace.

Lisa also practises in the area of privacy, cybersecurity and information management, advising both Canadian and international clients on compliance with Canadian privacy requirements. She routinely advises clients on trans-border data transfers, data breach management and anti-spam compliance. She also advises on the oversight obligations of boards of directors regarding cybersecurity issues and on cybersecurity risk mitigation strategies more generally.

Lisa is a prolific writer on technology, privacy and cybersecurity law issues, including as the author of the monthly "IT Girl" column for Canadian Lawyer magazine online. She has contributed to such publications as the American Bar Association (ABA)'s Business Law Today, Internet and E-Commerce Law in Canada and e-Commerce Law Report and has spoken for the ABA, Lexpert, the Canadian Technology Law Association, the Ontario Bar Association and the International Technology Law Association.

Lisa has been highly recognized by for her technology and privacy law expertise both nationally and internationally. She was awarded the 2018 Lexpert Zenith Award for Mid-Career Excellence in Computer and IT Law. She has been recognized since 2015 by *The Best Lawyers in Canada* for Privacy and Data Security Law, Technology Law; has been ranked in *Chambers Canada* and *Chambers Global* for Information Technology; and as a recommended lawyer in Computer & IT Law in *The Canadian Legal Lexpert® Directory* since 2005. She holds leadership positions in the ABA's Business Law and Science and Technology Sections.

Robert Lord
Chief Security Officer
Democratic National Committee

Robert Lord is the Chief Security Officer for the Democratic National Committee and leads the committee's cybersecurity operations. Mr. Lord works with the organization's own internal security team as well as in the field to support state parties, including efforts to update their "information security strategies" and improve practices to "change the economics" for would be cyber-attackers.

Michele Lucan

Assistant Attorney General
Connecticut Office of the Attorney General

Michele Lucan is an Assistant Attorney General at the Connecticut Attorney General's Office in its Privacy and Data Security Department. In this role, Michele handles all matters involving consumer privacy and information security. Most notably, Michele is currently leading and/or co-leading multistate investigations of several massive data breaches involving sensitive personal information.

Michele joined the Attorney General's Office in 2008 and first served in its Consumer Protection Division, where she investigated and pursued enforcement actions against a variety of unfair and deceptive business practices under the Connecticut Unfair Trade Practices Act. In 2013, Michele was appointed to a multidisciplinary Privacy Task Force that was created to focus the Office's response to privacy concerns and data breaches, and educate the public and Connecticut businesses about data protection responsibilities under state and federal law. In early 2015, a dedicated Privacy and Data Security Department was formed and Michele was assigned full-time to the Department from its inception. Michele has spent the past several years working exclusively on privacy-related matters.

Michele is a Certified Information Privacy Professional (CIPP)/ U.S. She received her B.A. from Loyola University in Maryland and her J.D. from the Quinnipiac University School of Law. Michele speaks regularly on privacy-related topics to government, bar and industry groups.

CHRISTINE E. LYON

Partner, Morrison & Foerster LLP

(650) 813-5770; clyon@mofo.com

Christine Lyon advises organizations on cutting-edge issues related to the collection, use, sharing, and safeguarding of data, including personal information of customers and employees. She serves as a trusted advisor, working with clients to develop global strategies to comply with U.S. and international privacy and data protection laws.

Christine's practice spans a variety of industry sectors, from information technology services to consumer products, and covers clients ranging from start-ups to large multinationals. She advises technology companies on building privacy protections into their offerings, including connected products and services (Internet of Things), cloud-based and mobile services, and social media initiatives, as well as on managing the related "Big Data" implications. She also assists clients in evaluating and managing privacy risks, including in strategic transactions such as IT outsourcing, and mergers and acquisitions.

Legal 500 US recognized Ms. Lyon as a "rising star" in the area of privacy and data protection and recommended her for cyber law, and she received The Burton Award for Distinguished Legal Writing. She frequently writes and speaks on the topics of global data protection laws, workplace privacy issues, and data security laws. She is a co-editor of *Global Employee Privacy and Data Security Law* (BNA Books) and a member of the editorial board of the World Data Protection Report.

Aristedes Mahairas

Special Agent in Charge, Counterintelligence/Cyber Division
Federal Bureau of Investigation (NYC)

Aristedes Mahairas, Special Agent in Charge, heads the New York (NY) Counterintelligence/Cyber Division. He previously served as Legal Attache, Athens; Joint Terrorism Task Force Supervisor; Section Chief, Strategic Operations Section-Counterterrorism Division; Chief of Staff to the Executive Assistant Director, National Security Branch. He previously served as a Police Officer in NY City and received a Bachelor's of Arts degree in Political Science-Baruch College, and a Juris Doctor-NY Law School.

Patrice Malloy
Bureau Chief
Florida Office of the Attorney General

Patrice Malloy is Bureau Chief at the Florida Office of the Attorney General leading the Multistate and Privacy Bureau where she manages a wide range of cases and investigations including Privacy and Data Breaches. As an executive committee member, she pursued investigations and settlements against several Pharmaceutical, Automobile and Telecommunication companies for violations of Florida's Unfair and Deceptive Trade Practices.

Ms. Malloy worked on one of the first multistate data breach cases initiated in 2007, that led to a settlement with the TJX Companies, Inc. which includes Marshalls, TJ Maxx and HomeGoods stores. Ms. Malloy participated on the Multistate Executive Committees' privacy and data security investigations into Uber, Target, Nationwide, and Google Safari and Google Street View. Most recently she settled a social media case against Devumi that involved the use of bots to generate and create endorsements. Ms. Malloy held a leadership position in the national Risperdal Pharmaceutical investigation and settlement.

Ms. Malloy served as faculty for continuing legal education and conferences including Practicing Law Institute's Annual Institute on Privacy and Data Security Law, NAAG's Anatomy of Complex Civil Litigation, and International Association for Privacy Professionals' Global Privacy Summit. She is a Certified Information Privacy Professional (CIPP/US).

Ms. Malloy worked in private practice for a major Miami law firm before joining the Florida Attorney General's office. Prior to practicing law, she worked as an anchor, reporter, and producer for CBS affiliated stations in Southwest Florida and St. Louis, Missouri where she handled complex consumer investigations and trial coverage. She is the recipient of state and national reporting awards, including Dartmouth's Champion Tuck Award and a Florida Bar Award for trial coverage.

Following her undergraduate education from Temple University in Philadelphia, Ms. Malloy earned a Masters' in Business Administration from the University of Missouri and a law degree from the University of Miami.

Lesley Matty
Tiffany & Co.

Lesley Matty is Senior Counsel - Intellectual Property & Global Data Privacy for Tiffany & Co., responsible for intellectual property, data privacy, advertising, media and PR matters, as well as related retail and corporate matters worldwide. Prior to joining Tiffany, Lesley was Legal Counsel at Richemont North America, Inc., which owns several of the world's leading luxury watch and jewelry brands. At Richemont, Lesley managed domestic intellectual property enforcement for all brands and a wide variety of transactional matters. Before moving in-house, Lesley was an associate at two boutique intellectual property firms where her practice focused on domestic and international trademark and copyright clearance, prosecution, portfolio maintenance, enforcement and litigation. She is a graduate of Emory University and Yeshiva University's Benjamin N. Cardozo School of Law.

Laura Juanes Micas

Global Director, Privacy Policy Engagement
Facebook

Laura Juanes Micas is a multilingual law, policy and privacy expert in the technology industry. She currently serves as Global Director of Privacy Policy Engagement at Facebook Inc.

Laura is a Spanish qualified lawyer, based in the United States, with more than fifteen years of professional experience in technology and media companies. In her role at Facebook, she leads a global team that regularly engages with regulators, policymakers, experts and advocates in order to inform on key privacy issues that impact how individuals use or relate to Facebook’ s technology daily. Prior to joining Facebook, she served as an Assistant General Counsel, Privacy & Human Rights, at Yahoo Inc., where she led the legal and public policy team’s efforts on global privacy matters and the company’s Business and Human Rights Program.

Before assuming her AGC role at Yahoo, Laura held various positions, including as General Counsel at Yahoo Spain and as Director of Product Compliance and Law Enforcement response for the Americas. Laura is a law graduate of the Universidad Autónoma de Madrid, where she worked as a lawyer before joining Yahoo.

Laura holds U.S. and EU Certifications for International Privacy Professionals (CIPP). She serves on the Advisory Board of the Information Accountability Foundation and chairs the Latin America chapter of the Centre for Information Policy Leadership. She is a mentor of startups and entrepreneurs in South Florida and Latin America and a proud Board and founder Member of Woman in Tech Miami Council, with a mission to connect and empower women with diverse technological backgrounds.

William E. Min

Deputy General Counsel & Chief Privacy and Data Governance Officer
Western Union Company

Bill Min is Deputy General Counsel & Chief Privacy and Data Governance Officer for Western Union where he leads the company's global privacy and information governance organization.

Prior to Western Union, Bill was Senior Vice President, Legal and Chief Privacy Officer at Live Nation Entertainment, Inc. He also worked for 16+ years at Starwood Hotels & Resorts Worldwide, Inc. where he led several global functions, including privacy, enterprise risk management, and operational compliance. Among his accomplishments, Bill is acknowledged as an expert in the area of data privacy, and established the global privacy function at both Live Nation and Starwood. Earlier in his career, Bill held in-house legal positions at Sara Lee Corporation and at Sunkyong America, Inc., the US subsidiary of one of the largest Korean conglomerates. Prior to working as in-house counsel, Bill was a mergers and acquisitions attorney at two New York City law firms.

Bill earned his Bachelor of Arts degree from the University of Pennsylvania, his Master of Arts degree from the State University of New York at Stony Brook, and his Juris Doctor degree from Fordham University School of Law.

Maneesha Mithal

Associate Director
Division of Privacy and Identity Protection
Federal Trade Commission

Maneesha Mithal is the Associate Director of the Federal Trade Commission's Division of Privacy and Identity Protection, which focuses on consumer privacy, data security, and credit reporting issues. In this capacity, she has managed significant initiatives, including reports on Big Data, the data broker industry, the Internet of Things, consumer privacy, facial recognition, and mobile privacy disclosures. She has testified before Congress on data security, connected cars, facial recognition, and identity theft. She has also supervised Commission investigations that resulted in consent orders, including against companies such as Wyndham, Google, Facebook, Twitter, Lifelock, HTC, Snapchat, Uber, and Lenovo. She has held numerous positions at the Commission, including Chief of Staff of the Bureau of Consumer Protection, and Assistant Director of the International Division of Consumer Protection. Prior to joining the Commission in 1999, Ms. Mithal was an attorney at the Washington law firm of Covington & Burling. Ms. Mithal earned her law degree from the Georgetown University Law Center and her undergraduate degree from Georgetown University.

Alejandro Mosquera

Director and Assistant General Counsel, MUFG

Alejandro Mosquera is data attorney at MUFG and is based in New York. He is responsible for providing legal advice in connection with data processing activities (including data privacy and data protection) affecting MUFG's global operations. Alejandro holds a J.D. from the *Universidad de los Andes*, an M.I.A. in International Finance and Management from Columbia University, an L.L.M. from The University of Chicago Law School and a one-year course diploma on International, Comparative and European Law from the *Université Robert Schuman*. Alejandro is admitted to practice law in New York and Colombia and is a Certified Information Privacy Professional (US) and Certified Information Privacy Manager. He is fluent in Spanish, English, Portuguese, Italian and French.

Marty Myers

Covington & Burling LLP

mmyers@cov.com

Martin H. (Marty) Myers is a partner in the firm's San Francisco office and a member of the Insurance Coverage and Arbitration practice groups, representing corporate policyholders in complex coverage disputes with their insurers.

A nationally recognized insurance recovery practitioner, Mr. Myers has helped clients recover billions of dollars in a wide array of industries, from agriculture to technology.

For more than twenty years, he has litigated, arbitrated and resolved complex coverage disputes throughout the world over a variety of losses and claims, including media liability, intellectual property, product recall, catastrophic property and business income loss, securities fraud and derivative litigation, management and professional liability, marine cargo, crime, alien tort/torture victim protection act, employment practices, mass tort and long tail asbestos and environmental claims. Mr. Myers routinely advises clients on insurance program placement and complex risk transfer and indemnification issues; he is regarded as one of the world's leading lawyers in transaction risk insurance products, including representation and warranty (warranty and indemnity) and tax loss insurance.

Representative Matters

- Represented The Walt Disney Company in several insurance arbitrations in the US and Canada regarding coverage for major media liability/defamation, employment practices and class action matters.
- Represented Adobe Systems, Inc. in successful litigation in Northern District of California to obtain defense fees/costs and indemnification under errors and omissions policies for massive exposure in font rights and misappropriation litigation brought by Agfa Monotype (originator of Times New Roman font).
- Represented Sony Computer Entertainment America in obtaining substantial recovery through insurance litigation in Northern District of California and U.S. Court of Appeals for the Ninth Circuit for losses from consumer class actions for alleged damages associated with Sony PlayStation® game consoles.
- Represented the GIC, the Government of Singapore real estate sovereign wealth fund in successful litigation and arbitrations recovering full first party and third party policy proceeds for loss of warehouse storage facilities by fire outside of Seoul, and follow on liabilities to third party property owners and others.
- Represented the E. & J. Gallo Winery and glass bottle-making affiliate in successful insurance litigation for recovery of losses from first party and third

party insurers for property damage and business income losses arising from catastrophic failure or glass furnace.

- Represented IAC/InterActiveCorp in obtaining substantial recoveries under errors & omissions policies for defense and settlement of consumer class actions over TicketMaster “Entertainment Rewards” programs; also advised IAC on errors and omissions and general liability coverage for match.com consumer class actions.
- Represented World Fuel Services in litigation in Southern District of New York obtaining complete recovery, plus interest under marine cargo policy for phishing theft of millions of tons of marine gas oil lost to pirates off the coast of Togo.

Accolades

- *Law360*, Insurance MVP (2016)
- *Chambers USA*, Insurance: Policyholder
- *The Best Lawyers in America*, Insurance Law (2014-2018)
- *The Legal 500 US*

Education

- University of Michigan Law School, J.D., 1987
- Miami University, B.A., 1984

Bar Admissions

- California
- Numerous admissions *pro hac vice* throughout the United States
- Has appeared for clients in marine matters in Courts of Norway

Kirk Nahra

WilmerHale

PH: 202-663-6128; Email: KIRK.NAHRA@WILMERHALE.COM

Kirk Nahra has been a leading authority on privacy and cybersecurity matters for more than two decades. Indeed, he is one of the few lawyers in the world ranked in Band 1 by *Chambers* in privacy and data security. Mr. Nahra counsels clients across industries, from Fortune 500 companies to startups, on implementing the requirements of privacy and data security laws across the country and internationally. He also advocates for clients experiencing privacy and security breaches, and represents clients in contract and deal matters, enforcement actions, regulatory investigations and related litigation.

Mr. Nahra is best known for his work with health insurers, hospitals, service providers, pharmaceutical manufacturers and other health care industry participants. He has a deep understanding of the privacy and security issues healthcare companies face relating to HIPAA rules, state and federal legislation, enforcement activities, internal investigations, international principles, due diligence in transactions, data breach risk assessments, and the key lines between regulated and unregulated data. During his decades of experience, Mr. Nahra has developed compliance programs, drafted privacy and information security policies, negotiated agreements involving health data, responded to health incidents and defended clients against government investigations.

Mr. Nahra also has substantial experience working with clients in the financial services and insurance industries on privacy and data security matters relating to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Fair and Accurate Credit Transactions Act, data aggregation and sharing practices, and privacy and data security compliance under a wide range of state and federal laws. He also has a breadth of experience drafting and evaluating data security practices and policies across varying industry standards; has investigated and litigated potential fraud against insurers, and has assisted with the development and oversight of corporate compliance programs.

Professional Activities

A leader in the privacy bar, Mr. Nahra has been involved in developing the privacy legal field for 20 years. As a founding member and current board member of the International Association of Privacy Professionals, he helped establish the organization's Privacy Bar Section and their first and most popular certification for Certified Information Privacy Professionals. He has taught privacy issues at several law schools, including serving as an adjunct professor at the Washington College of Law at American University and at Case Western Reserve University. In addition, he currently serves as a fellow with the

Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis and as a fellow with the Institute for Critical Infrastructure Technology. He actively shares his privacy insights through numerous speeches and articles, and on social media.

Solutions

Cybersecurity and Privacy

Credentials

EDUCATION

JD, Harvard Law School, 1987
cum laude

Articles Editor, Harvard Journal on Legislation

BA, Georgetown University, 1984
magna cum laude Phi Beta Kapp

ADMISSIONS

District of Columbia

Aimee Nolan
W.W. Grainger, Inc.

Aimee Nolan is the Vice President, Associate General Counsel and Chief Intellectual Property Counsel for W.W. Grainger, Inc. She is responsible for litigation matters as well as all aspects of Grainger's Intellectual Property portfolio, including patents, trademarks, copyrights and domain names. Aimee also supports the company's Enterprise Systems organization as well as global product sourcing, marketing and corporate communications. She is also a leader of Grainger's enterprise wide efforts on data protection, data security, privacy and breach response.

Aimee has also served as primary legal counsel to several Grainger business units and has advised in the areas of corporate and commercial law, securities, bankruptcy, credit and collections, customer and supplier agreements and services. She has extensive experience working on large, complex projects and has successfully supported many strategic company initiatives. Aimee has been at Grainger since 1998.

Aimee is a member of the Chicago and American Bar Associations, American Intellectual Property Association, Intellectual Property Law Association if Chicago (IPLAC), International Association of Privacy Professionals (IAPP), Association of Corporate Counsel (ACC), and the International Trademark Association (INTA). Aimee is a member of the In-House Advisory Committee of ChiWIP (Chicago Woman in IP). She is also an Executive Member of the Board of Directors of the Judd Goldman Adaptive Sailing Foundation and co-chaired their annual fundraising gala in 2014, 2015 and 2016. She is a 2015, 2016 and 2018 First Chair Award Recipient. Aimee is also a member of the Board of the Illinois Chapter of the Alzheimer's Association and chairs the Illinois Woman Conquer Alz! Steering committee.

Kathleen M. Porter

Robinson & Cole LLP

Tel: 617-557-5989; Email: kporter@rc.com

Kathleen Porter is an intellectual property and technology partner in the Business Transactions Practice Group, and former chair of the firm's Intellectual Property and Technology Practice. Her practice straddles the areas of intellectual property, business transactions, data privacy and trade regulation.

International

Ms. Porter regularly counsels international companies on their entry and expansion into the U.S. market, including selecting an entity, coordinating employment terms and visas applications, "Americanizing" standard agreements and coordinating introductions to insurance, leasing, PEO and other service providers.

Privacy

Ms. Porter counsels organizations on the development and implementation of data security and privacy practices to comply with the patchwork of laws and rules applicable to the collection, use, safeguarding, sharing, and transfer of protected or personal data. She regularly structures arrangements with promoters, marketers, website exchanges, and other third parties for the purchase, sale, sharing, and safeguarding of personal data. Ms. Porter prepares and negotiates representations, warranties, and indemnities regarding personal or protected data and privacy and data practices for commercial and M&A transactions. She assists clients with privacy audits and works with third-party certification organizations to obtain certification of the organization's privacy practices. She guides clients through internal investigations to assess and address notice and other obligations regarding privacy breaches. Ms. Porter often works closely with our litigation attorneys to manage external investigations such as those by federal or state regulators.

Intellectual Property; Information Technology

Ms. Porter counsels clients on the development, protection, and commercialization of intellectual property and technology. In particular, online contracting, electronic signatures, mobile applications, online promotions and testimonials and electronic signatures. She also has significant experience negotiating U.S. and cross border commercial agreements, including distribution, SaaS, representative, manufacturing, licensing, development, outsourcing, services, BPO, systems and software acquisitions and equipment leasing arrangements, technology support and maintenance, strategic alliances, and other collaboration agreements.

Alan Charles Raul

Partner, Privacy and Cybersecurity Practice

Sidley Austin LLP

PH: 202-736-8477; Email: araul@sidley.com

ALAN RAUL is the founder and leader of Sidley's highly ranked Privacy and Cybersecurity practice. He represents companies on federal, state and international privacy and cybersecurity issues, including digital governance, global data protection and compliance programs, data breaches, consumer protection issues and Internet law. Alan advises companies regarding their cybersecurity preparedness and helps them manage data security incidents. His practice involves litigation and counseling regarding consumer class actions and investigations, enforcement actions and policy development by the FTC, State Attorneys General, SEC, Department of Justice, financial regulators, EU Data Protection Authorities, and other government agencies.

He regularly represents leading tech, telecom, media, financial services and other companies with respect to their digital governance, compliance and crisis management. Alan has recently represented a special cybersecurity review committee of the Board of Directors of a major tech company in connection with its independent investigation of the company's handling of significant data breaches.

Alan provides clients with perspective gained from extensive government service. He previously served as Vice Chairman of the White House Privacy and Civil Liberties Oversight Board, General Counsel of the Office of Management and Budget, General Counsel of the U.S. Department of Agriculture, and Associate Counsel to the President.

Alan serves as a member of the Technology Litigation Advisory Committee of the U.S. Chamber Litigation Center (affiliated with the U.S. Chamber of Commerce). He also serves as a member of the American Bar Association's Cybersecurity Legal Task Force by appointment of the ABA President, and as a member of the Practicing Law Institute's (PLI) Privacy Law Advisors Group.

Alan is a member of the governing Board of Directors of the Future of Privacy Forum. He is a member of the Center for Democracy and Technology's Advisory Committee. Alan also serves on the Executive Committee of the Federalist Society's Administrative Law Practice Group. Alan is a frequent author and speaker on privacy, cybersecurity and related issues. He is overall editor arid a contributing

author of *The Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd, 5th ed. 2018).

Alan holds degrees from Harvard College (AB *magna cum /aude),* Harvard Kennedy School of Government (MPA), and Yale Law School (JD). He clerked for Judge Malcolm R. Wilkey of the U.S. Court of Appeals for the D.C. Circuit.

Adam Rivera
Refinitiv
Adam.Rivera@refinitiv.com

Adam Rivera leads the privacy team for the Americas region at Refinitiv, formerly the Financial & Risk business of Thomson Reuters. Adam is also the primary attorney at Refinitiv that supports the company's cybersecurity program. Adam was heavily involved in the company's GDPR readiness program. Adam is also leading compliance and advocacy efforts related to the newly enacted data privacy laws in California and Brazil. Prior to his current role, Adam held various positions at Thomson Reuters, Louis Vuitton and practiced at Schulte Roth & Zabel LLP.

Alexandra Ross

Director, Global Privacy and Data Security Counsel
Autodesk, Inc.

Alexandra Ross is Director, Global Privacy and Data Security Counsel at Autodesk, Inc., a leader in 3D design, engineering and entertainment software. Previously she was Senior Counsel at Paragon Legal and Associate General Counsel for Wal-Mart Stores. She is a certified information privacy professional (CIPP/US, CIPP/E, CIPM, CIPT and FIP) and practices in San Francisco, California. She holds a law degree from Hastings College of Law and a B.S. in theater from Northwestern University. Alexandra is a recipient of the 2019 Bay Area Corporate Counsel Award – Privacy.

Alexandra launched The Privacy Guru blog in January of 2014 and has published an ebook *Privacy for Humans* (available on Amazon and iTunes).

Rachel Roy

Associate General Counsel, Global Employment and Compliance
Sensata Technologies

Rachel Roy is Associate General Counsel, Global Employment and Compliance for Sensata Technologies, Inc., a 22,000-employee multinational supplier of sensing, electrical protection, and power management solutions based in Attleboro, Massachusetts. Ms. Roy manages Sensata's global employment law practice and serves as a legal partner to the Company's compliance function, including advising in the areas of internal investigations, business ethics, anti-corruption/anti-bribery, data privacy, and general regulatory compliance.

Prior to joining Sensata, Ms. Roy was Senior Legal Counsel for Re:Sources USA, a Publicis Groupe Company, focusing on employment law (including employee relations, internal investigations, employee cross-border and mobility issues, harassment, discrimination, pay equity, employment disputes, and reductions in force). Ms. Roy also has extensive litigation experience. She began her career with Jackson Lewis PC where she represented management in complex employment litigation matters before state and federal courts, as well as administrative agencies.

Ms. Roy holds a B.A. in Economics from Brandeis University and a J.D. from Suffolk University Law School.

Clark Russell

New York State Attorney General's Office

Clark Russell is the Deputy Bureau Chief of the Bureau of Internet and Technology at the New York State Attorney General's Office. The Bureau is committed to protecting consumers from online threats and has brought a number of ground-breaking cases involving internet and technology issues, including privacy, online fraud and data security. Clark's investigations included Secure Our Smartphones, where the office convinced smartphone manufacturers to install a "kill switch" in their smartphones; and Operation Clean Turf, the largest investigation into companies flooding the Internet with fake positive reviews; Operation Child Tracker, the largest state AG investigation of violations of the Children's Online Privacy Protection Act ("COPPA") by major child brand websites, and a well-known ad network. Clark oversees the office's data breach notification program, and secured numerous record-setting results in data breach cases. He is also the principal draftsperson of the office's proposed overhaul of New York State's data security law to require new and unprecedented safeguards of personal data.

Al Saikali
Shook, Hardy & Bacon L.P.P.

Al Saikali is a *Chambers*-ranked lawyer specializing in privacy and data security law. In addition to chairing Shook, Hardy & Bacon's Privacy and Data Security practice, he founded and chairs the Sedona Conference's Working Group on Privacy and Data Security Liability, and co-chairs the American Bar Association's Cybersecurity Law Institute. He has won the *Lexology* Client Choice award in technology law the last two years in a row and was named a "Trailblazer in Cybersecurity" by the *National Law Journal* in 2015. In his spare time, Al is an Adjunct Professor at Saint Thomas University where he teaches Cybersecurity Law, and he maintains a blog (Data Security Law Journal) where he writes about emerging trends and issues in privacy and data security law. Al has been quoted by the *Wall Street Journal*, *Bloomberg BusinessWeek*, and *Law360* for his thoughts on privacy and data security legal trends.

Andrew Sawyer
Director of Security
Locke Lord LLP

Andrew Sawyer is responsible for all aspects of physical and cyber security at Locke Lord.

Prior to joining the firm, he had a long-term career with the National Football League (NFL) working as a technology director, for three NFL teams and for European operations. Andy is a member of the FBI Infragard partnership with the private sector and the Greater Houston Partnership Cybersecurity Task Force.

Aaron P. Simpson

Hunton Andrews Kurth LLP

ASimpson@HuntonAK.com; 212.309.1126, +44 (0) 20 7220 5612

Aaron Simpson is a partner with Hunton Andrews Kurth and head of the firm's EU data protection and privacy practice. He advises clients on a broad range of complex privacy, data protection and cybersecurity matters, including international and U.S. federal and state privacy and data security requirements. Aaron's work ranges from advising clients on large-scale cybersecurity incidents to the development of cross-border data transfer solutions, compliance with existing and emerging data protection requirements in Europe, and negotiating data-driven commercial agreements. He has advised numerous clients on the EU General Data Protection Regulation (GDPR). He also prepares proactive, data breach-readiness solutions for clients, including through the creation of incident response plans and conducting board-level tabletop exercises.

Aaron is well known as a top privacy professional and has been recognized by Chambers and Partners, Computerworld and The Legal 500 for his work on behalf of clients. Aaron is the only lawyer listed in both *The Legal 500 United Kingdom* and *The Legal 500 United States* guides, providing clients with a broad and unique transatlantic perspective on privacy, data protection and cybersecurity matters.

In addition, Aaron is a sought-after media resource on privacy issues and has been quoted in such publications as *Bloomberg BNA, Businessweek Magazine, Computer Weekly, Corporate Secretary, DataGuidance, Law360, SC Magazine, The Times and TIME Magazine*. He regularly speaks before industry groups, legal organizations, government agencies and educational institutions at conferences, seminars, roundtables and webinars. He has written and co-written numerous articles, book chapters and handbooks on privacy and information security issues.

Aaron received his JD from the University of Virginia School of Law and his BA from the University of Texas, High Honors. He is admitted to practice in New York, and is a Registered Foreign Lawyer of England and Wales.

Jason N. Smolanoff

Senior Managing Director, Global Practice Leader, Cyber Risk, Kroll

jason.smolanoff@kroll.com – phone: 213-443-6055

Jason Smolanoff is a senior managing director, Global Cyber Risk Practice Leader, based in the Los Angeles office. Jason, who brings more than 16 years of federal law enforcement and information security experience, has played a leading role in some of the most significant cyber security investigations in history. Over his career, he has specialized in supervising and investigating sophisticated computer and network intrusions conducted by state-sponsored organized crime, hacktivists, and insider threat actors, often developing and maintaining productive partnerships with international intelligence and law enforcement agencies as well as private industry.

Prior to joining Kroll, Jason was CEO of CISO Advisory & Investigations LLC, a firm he founded in 2015 to provide a wide range of outsourced information security services to publicly traded and private corporations, including their corporate boards and c-suite members. Concurrently, he has been serving as a Commissioner for the San Manuel Gaming Commission in Highland, California, a position he continues to hold.

From 2011 to 2015, Jason was a Managing Director in the Los Angeles office of Stroz Friedberg. In addition to business development responsibilities, Jason led engagements for over 100 matters touching all of the firm's business units, including digital forensics, incident response, security risk assessments, and investigations. During this time, he also developed a profitable content protection and anti-piracy service offering for the firm.

Jason entered the private sector after serving with the FBI from 1999-2011, primarily from the Los Angeles field office. Most recently, he was the Supervisory Special Agent for the Cyber National Security Squad, where he supervised 12 Special Agents and Intelligence Analysts in responding to all aspects of complex cyber national security investigations with a nexus to counterintelligence and counterterrorism matters.

Before entering law enforcement, Jason was a physical chemist employed by a major semi-conductor equipment manufacturer, where he specialized in facilitating the manufacture of cutting-edge computer chip technology for clients such as IBM, Intel, Motorola, Philips, Sony, and Lucent. His innovative leadership and solutions earned him two U.S. patents.

A noted authority in cyber-related matters, Jason is an Adjunct Professor with the Loyola Law School, as well as a member of Loyola's Cybersecurity and Data Privacy Advisory Group. Jason has also often served as keynote speaker and delivered numerous presentations before a wide range of industry, academic, government, and corporate audiences around the world.

JAMES G. SNELL
Perkins Coie

Jim Snell is a partner in the Privacy & Security Group at Perkins Coie. He represents clients in a broad range of complex commercial matters, including Internet and privacy issues, security issues, IP, false advertising, and class actions. Jim's experience includes, among other things, IoT, unmanned vehicles, wiretap and surveillance matters, AI and machine learning, the Communications Decency Act, biometrics, web scraping, data breach, and the Telephone Consumer Protection Act.

Jim is a Certified Information Privacy Professional (CIPP) as designated by the International Association of Privacy Professionals (IAPP).

Jacob Springer
Abbott Laboratories

As the Global Privacy Lead and Division Counsel at Abbott Laboratories, Jacob leads the company's privacy program and supports Abbott's global businesses as Chief Privacy Counsel.

Jacob has 15 years of experience in leading global privacy programs for Fortune 100 companies. He has completed law degrees from Europe/Austria and the US/University of Virginia. Prior to joining Abbott, Jacob served at Baxter International as Global Privacy Officer. Additionally, Jacob supported Europe, Canada and Latin America as general compliance counsel gaining over ten years of broad compliance management experience.

During his tenure at Abbott and Baxter, Jacob provided counsel to executive management on an ongoing basis to ensure the companies' privacy and data protection programs were aligned with business priorities and strategy. Additionally, Jacob also led efforts to ensure product and process development were aligned with privacy and data protection requirements of consumers and regulators globally.

Jacob's qualifications include:

- Member of the New York Bar
- Fellow of Information Privacy [FIP]
- Certified Information Privacy Professional – US [CIPP US]
- Certified Information Privacy Professional – Europe [CIPP E]
- Certified Information Privacy Professional – Canada [CIPP C]
- Certified Information Privacy Manager [CIPM]
- Certified HIPAA Professional [CHP]
- IPPC [International Pharmaceutical Privacy Consortium] board member
- MDPC [Medical Device Privacy Consortium] chair, vice chair and board member

Zoë Strickland

Vice-President, Global Privacy & US Commercial Compliance
Cigna

Zoe Strickland is the newly appointed VP, Global Privacy & US Commercial Compliance head for Cigna health and life insurance. She most recently served as the Managing Director, Global Chief Privacy Officer, for JPMorgan Chase, where she was responsible for domestic and global privacy compliance at the company enterprise level, including its privacy policies, procedures, governance, strategy, training, and administration. Previously, Zoe served as the VP, Chief Privacy Officer for UnitedHealth Group and for Walmart Stores Inc.

Zoe is an active participant in the privacy community. She serves on the Advisory Board of the Future of Privacy Forum and several other cross-industry organizations. She previously served on the Board of Directors for the International Association of Privacy Professionals (IAPP). Zoe is a frequent speaker at industry conferences and events, has testified before subcommittees of the House Energy and Commerce Committee, and has been quoted in national and trade media sources, including USA Today, the New York Times, and National Public Radio.

Matthew W. Van Hise
Assistant Attorney General
Chief of the Privacy Unit
Illinois Attorney General's Office

Matthew W. Van Hise is an Assistant Attorney General and Chief of the Privacy Unit at the Illinois Attorney General's Office. AAG Van Hise has been with the Attorney General's Office working in the Consumer Fraud Bureau since 2011. He enforces the Illinois Consumer Fraud and Deceptive Business Practices Act and spends the majority of his time focusing on privacy, data security, and data breach related investigations and litigation. AAG Van Hise functions as both the lead and co-lead attorney for many national multistate investigations into several of the largest data breach incidents to date.

As Chief of the Privacy Unit, he serves as the point person within the Illinois Attorney General's Office on matters such as privacy, data security, technology, and the secure handling of consumers' personal information. AAG Van Hise also oversees the Illinois Attorney General's Identity Theft Unit, which was created in 2006 and has assisted over forty-five thousand consumers with complaints covering a wide variety of identity theft issues and privacy areas.

Matthew leads the National Association of Attorneys General Privacy Working Group, on both privacy and identity theft. He also co-leads the NAAG medical privacy discussions.

Prior to this, he worked at the Michigan Attorney General's Office, on both privacy and identity theft. Matthew received a B.A. from Bradley University and a J.D. from the Thomas M. Cooley Law School in Lansing, Michigan. Matthew has served as panelist and as guest speaker at numerous data security and privacy conferences throughout the country. He is an active member in the International Association of Privacy Professionals, holding the CIPP/US certification, as well as a member in many local, state, and national Bar Associations.

Ryan Vinelli

Vice President, Privacy and Technology counsel
Western Union

Ryan Vinelli is a Vice President, Privacy and Technology counsel at Western Union. Western Union is a global leader in cross-border, cross-currency money movement. His work focuses on data protection, information security and ensuring a global-approach to securing data.

Prior to joining Western Union, Ryan was Global Cybersecurity Counsel for Verizon Media supporting brands including Yahoo, Aol, Tumblr, Huffington Post, Techcrunch and Engagdet. Ryan was also a Vice President handling global legal and privacy matters for Starwood Hotels & Resorts Worldwide, Inc. and after its acquisition at Marriott Hotels International. Ryan began his career in data protection as privacy counsel for General Electric.

Ryan is a graduate of the Benjamin N. Cardozo School of Law and holds undergraduate and graduate degrees in computer science from Tufts University. Ryan is licensed to practice law in multiple states and is a registered Patent attorney.

Michelle Visser

Partner, Orrick Herrington & Sutcliffe LLP

San Francisco, Boston

PH: 415-773-5518; Email: mvisser@orrick.com

Michelle Visser has extensive experience in defending companies that face the regulatory investigations, class action litigation, and payment card brand claims that frequently follow the announcement of cybersecurity incidents. In addition to litigating privacy and cybersecurity matters, Michelle has navigated numerous companies through their cybersecurity response, including by overseeing technical forensic investigations, advising on notification obligations and coordinating communication strategies.

When faced with an incident, companies call Michelle for crisis response with an eye toward potential litigation. Clients also look to Michelle for privacy and cybersecurity advice before a crisis is at hand. Michelle regularly takes the lessons learned from litigating privacy and cybersecurity matters to provide clients with proactive advice on how to structure their privacy and cybersecurity programs and incident response plans in ways designed to reduce legal exposure.

For her role in representing companies that have faced some of the most high-profile cybersecurity incidents and litigation to date, Michelle was named one of the “40 Under 40” in 2018 by the *Global Data Review* and a “Rising Star” by *Law360* in 2015. She was also recognized as one of the “Women Leaders in Technology Law” by *The San Francisco Recorder* in 2015.

Michelle is also regularly turned to for defense against other types of class actions and complex litigation with experience in defending companies against securities, antitrust, and other commercial claims.

Hilary M. Wandall

General Counsel
Corporate Secretary and Chief Data Governance Officer
TrustArc

Hilary Wandall is General Counsel, Corporate Secretary and Chief Data Governance Officer of TrustArc Inc. She oversees all legal, regulatory and policy and strategic partnership matters and manages the legal, policy and data governance, regulatory affairs and business development teams. She also serves as President of the certification subsidiary, TRUSTe LLC. Hilary joined TrustArc in 2016 after 22 years at the global pharmaceutical company, Merck, where she most recently was AVP, Compliance and Chief Privacy Officer. Hilary led the global privacy program at Merck since 2004 and the global compliance program for the Merck Animal Health business since 2013. During her tenure at Merck, Hilary also held positions as corporate attorney, marketing promotion manager and biomedical research scientist.

Hilary is actively engaged in efforts to support the development of the privacy profession, to drive interoperability across privacy and data protection regimes around the world, and to scale and integrate privacy and data governance through technology. She recently has co-authored multiple articles on cross-jurisdictional privacy interoperability. She has been involved in various organizations across the privacy and legal communities, including the Executive Committee of the IAPP Board of Directors and 2016 IAPP Board Chairman, Chair of the Board of the International Pharmaceutical Privacy Consortium, member of the OECD Privacy Experts Working Group, Executive Committee of the Board of Trustees of the International Accountability Foundation, Advisory Board of the Future of Privacy Forum, Steering Committee of the Centre for Information Policy Leadership, and the Advisory Board of the Temple Law Center for Compliance and Ethics.

Hilary received her law degree and MBA from Temple University, Master of Bioethics from the University of Pennsylvania, and Bachelor of Science in Biology from Moravian College. She holds the CIPP/US, CIPP/EU and CIPM certifications. She is also a Fellow of Information Privacy. She is admitted to practice law in New Jersey and Pennsylvania. She resides with her family in Pennsylvania.

Ericka Watson
Danaher Corporation

Ericka Watson is Lead Counsel for Global Data Privacy & EU Data Privacy Officer at Danaher Corporation, a global science and technology innovator committed to helping customers solve complex challenges and improving quality of life around the world. She has strategic and tactical experience of implementing and enforcing comprehensive corporate privacy programs and cross-business working environments in the management of regulated data. She is responsible for leading the effort to develop and communicate Danaher's global data privacy compliance strategy, and advices Danaher and its operating companies on a wide range of business matters and strategies.

Ericka was previously a senior privacy leader at AbbVie, a global biopharmaceutical company, previously part of Abbott Laboratories. Prior to that she led privacy at GE Healthcare. She was responsible for leading global efforts to accomplish internal compliance and enabling client compliance with data protection requirements through the development of comprehensive and effective technology solutions, internal procedures, security controls, and awareness programs. She navigated challenging and novel privacy & data security issues and worked to develop compliant solutions.

Ericka is a frequent speaker on privacy matters including: Internet of Things, Big Data, GDPR, and Developing a Global Privacy Programs.

Ericka is currently serving as the Secretary of the American Bar Association Science and Technology Section. She received her BA from CUNY-Hunter College and earned her JD from the University of Wisconsin - Madison. She is currently an active member of the Illinois and Wisconsin Bar.

Jody R. Westby, Esq.
CEO, Global Cyber Risk LLC
westby@globalcyberrisk.com

Drawing upon a unique combination of more than twenty years of technical, legal, policy, and business experience, Ms. Westby provides consulting and legal services to public and private sector clients around the world in the areas of privacy, security, cyber governance, incident response, and digital asset inventories and data mapping. Her cyber risk assessment methodology has been used by large multinational corporations in nearly every industry sector. Her team has deep expertise in assessing industrial control and SCADA systems used in manufacturing, electrical grids, and critical infrastructure sectors. She also serves as Adjunct Professor to the Georgia Institute of Technology's School of Computer Science and is a professional blogger for *Forbes*.

Ms. Westby is a member of the bars of the District of Columbia, Pennsylvania, and Colorado. She serves as chair of the American Bar Association's (ABA) Privacy and Computer Crime Committee (Science & Technology Law Section) and co-chair of the Cybercrime Committee (Criminal Justice Section) and is serving a third term on the ABA President's Cybersecurity Task Force. She co-chaired the World Federation of Scientists' (WFS) Permanent Monitoring Panel on Information Security and served on the ITU Secretary-General's High Level Experts Group on Cybersecurity.

Ms. Westby led the development of the *International Toolkit on Cybercrime Legislation* and is an editor and co-author of the 2010 WFS-ITU publication, *The Quest for Cyber Peace*. Ms. Westby is co-author and editor of four books on privacy, security, cybercrime, and enterprise security programs and author of two books on legal issues associated with cybersecurity research, all published by the ABA. She speaks globally on these issues.

Previously, she launched In-Q-Tel for the CIA, was senior managing director at PricewaterhouseCoopers, was senior fellow and director of IT Studies for the Progress and Freedom Foundation, and was director of domestic policy for the U.S. Chamber of Commerce. Ms. Westby practiced law at Shearman & Sterling and Paul, Weiss, Rifkind, Wharton & Garrison. B.A., summa cum laude, University of Tulsa; J.D., magna cum laude, Georgetown University Law Center; Order of the Coif. Ms. Westby is a member of the American Bar Foundation and the Cosmos Club.

Dave Wong

FireEye Mandiant

dave.wong@mandiant.com

Dave Wong is a Managing Director at FireEye Mandiant. Mr. Wong manages the FireEye Mandiant cybersecurity consulting practice in North America. In this capacity, he leads and oversees projects to help organizations respond to cybersecurity incidents and make them more resilient to attack.

Mr. Wong has extensive experience in cybersecurity and investigating cybercrime. Over the past 10 years, he has investigated some of the largest cybersecurity incidents and provided evidence to help law enforcement arrest cybercriminals. Dave brings true front-line experience as he has visibility in the effectiveness of cybersecurity programs across many industries, and specifically what went wrong when companies suffer a cyber security incident. He uses this experience to help guide companies to secure their systems, data, and intellectual property.

Prior to joining FireEye, Mr. Wong was the Chief Operating Officer of the Intrepidus Group, a boutique cybersecurity firm that focused on mobile application and device security. Dave also worked at Bridgewater Associates, the world's largest hedge fund, as head of cybersecurity for the trading floor. He firmly believes that "it takes a thief to catch a thief", and started his career in cybersecurity conducting penetration testing to help companies identify computer security vulnerabilities.
Mr. Wong is a Certified Information Systems Security Professional (CISSP) and holds a degree in Engineering from the Cooper Union for the Advancement of Science and Art.

Stephen S. Wu
Shareholder
Silicon Valley Law Group
1 North Market Street, Suite 200
San Jose, CA 95113
(408) 573-5737
ssw@svlg.com

Stephen S. Wu is a shareholder with Silicon Valley Law Group in San Jose, California. He advises clients on transactions, compliance, liability, security, and privacy matters regarding the latest technologies in areas such as robotics, artificial intelligence, automated transportation, the Internet of Things, and Big Data. He helps clients with domestic and international privacy and security matters in negotiating agreements, incident response, breach notification, litigation, and managing privacy and security programs, certifications, and audits. He counsels clients concerning cyber-risk insurance policies and coverage and risk management strategies. In addition, he advises clients on secure electronic commerce using digital signatures, other secure electronic signatures, electronic credentials such as digital certificates, encryption, and public key infrastructure.

From 1997 to 2001, Mr. Wu was VeriSign, Inc.'s second in-house attorney, where he managed the development and deployment of worldwide policies and procedures for VeriSign's digital certification Internet security services. Before his work at VeriSign, he practiced with two international law firms in the areas of intellectual property and general litigation, as well as technology transactions.

Mr. Wu served as Chair of the American Bar Association Section of Science and Technology Law from 2010 to 2011. From 2001 to 2004, Mr. Wu was Co-Chair of the Section's Information Security Committee. He helped found the Section's Artificial Intelligence and Robotics, Internet of Things, Big Data, and Homeland Security Committees.

Mr. Wu has written or co-written seven books on information security law, including his most recent publications: *A Guide to HIPAA Security and the Law Second Edition* (2016) and *A Legal Guide to Enterprise Mobile Device Management: Managing Bring Your Own Device (BYOD) and Employer-Issued Device Programs* (2013). He has written numerous book chapters and articles on data protection, artificial intelligence, and robotics topics. He is a frequent speaker at industry conferences and continuing legal education programs on information security, EU's General Data Protection Regulation, artificial intelligence, robotics, autonomous driving, and other cutting edge technologies.

Mr. Wu received a Bachelor of Arts degree from the University of Pittsburgh in 1985, and graduated from Harvard Law School in 1988 with a Juris Doctor degree.

Miriam Wugmeister
Morrison & Foerster LLP

Few lawyers in the world have Miriam Wugmeister's breadth and understanding of privacy and data security laws, obligations, and practices. In the words of her clients, she is “extremely practical and phenomenally smart. Just about one of the best privacy advisers there is” (*Chambers USA*). Co-chair of Morrison & Foerster’s market-leading Global Privacy and Data Security Group and ranked among the top in the profession by all major directories, Ms. Wugmeister is regularly called upon by some of the world’s largest and most complex multinational organizations to confront their most difficult U.S. and international privacy challenges. “Tremendous at helping you come up with practical solutions to real problems” (*Chambers USA*), she develops cutting-edge solutions for clients that marry legal compliance with business realities.

Having helped hundreds of clients respond to data security incidents, Ms. Wugmeister has worked on several of the most noteworthy and largest data security incidents over the past few years. She has been praised as “clearly operating at the top of her profession; distinguished by her passion, ability to relate to clients, and practical business-minded advice” by *Legal 500*, which recently named Morrison & Foerster as the 2015 Cyber Crime Firm of the Year. Ms. Wugmeister also works with dozens of companies to develop comprehensive customized incident response plans, training staff, conducting extensive table top exercises, and addressing key issues with Boards of Directors and executive management.

Ms. Wugmeister advises organizations on the planning and execution of complex global compliance efforts, assists in the negotiation of strategic deals, and defends regulatory and litigation matters relating to privacy and data security in the U.S. and internationally. She serves as an arbitrator for the EU-US Privacy Shield Framework Binding Arbitration Program. Ms. Wugmeister regularly advises on data security breach issues; the global collection, use, sharing of employee, customer, vendor, and consumer personal information; ediscovery and monitoring conflicts; social media issues; and cloud computing deals, as well as on developing data security policies and procedures and cybersecurity preparedness and response plans. She also counsels clients on cutting-edge consumer privacy issues surrounding emerging technologies such as the Internet of Things (IoT), telematics, and big data.

As leader of the Global Privacy Alliance (GPA), Ms. Wugmeister encourages the rational development of privacy laws around the world and monitors privacy practices, laws, and regulations globally. On behalf of the GPA’s members, she takes an active role in anticipating upcoming privacy legislation and educating regulators on the commercial implications of proposed regulations. Ms. Wugmeister developed the firm’s Privacy Library and the MoFoNotes subscription database so that organizations can keep apprised of privacy and data security compliance requirements in jurisdictions around the world. She is also co-editor of *Global Employee Privacy and Data Security Law, Second Edition* (BNA Books, 2011).

Chambers USA and *Chambers Global* recommend Ms. Wugmeister in the top tier of privacy and data security lawyers worldwide, and *Legal 500 US* recognizes her as a leading lawyer for her "professionalism and strong international presence." For her work in data protection and privacy, Ms. Wugmeister is an inaugural inductee into the 2017 *Legal 500* Hall of Fame, which is comprised of outstanding U.S. lawyers who have been recommended as *Legal 500* "Leading Lawyers" for the last six consecutive years. In 2016, she was named one of *Financial Times'* "Top 10 Innovative Lawyers in North America" and a *National Law Journal* "Cybersecurity and Data Privacy Trailblazer" for her cutting-edge work in this space. Ms. Wugmeister was previously designated an *Ethisphere* "Attorney Who Matters," and a BTI Client Service All-Star, and has been featured in *Best Lawyers in America* every year since 2008.

Maureen A. Young

Senior Regulatory Counsel, Senior Vice President, Bank of the West

Maureen.Young@BankoftheWest.com

Maureen A. Young is Senior Regulatory Counsel and Senior Vice President at Bank of the West, a member of the BNP Paribas Group. She advises on a wide range of financial services regulatory, data privacy and security, compliance, examination, enforcement and corporate governance matters, as well as regulatory strategy and policy issues. She supports major business initiatives involving the Bank and its U.S. and global BNP Paribas affiliates, including innovation and fintech projects. She is a Certified Information Privacy Professional (CIPP/US), International Association of Privacy Professionals (IAPP).

Prior to joining Bank of the West in 2016, Maureen was Managing Director and Associate General Counsel at MUFG Union Bank, serving as a lead lawyer on key regulatory and implementation projects and as lead privacy counsel to the Privacy and Information Security team. The strategic projects she supported included strategy for and formation of a U.S. intermediate holding company as required by the Federal Reserve's Enhanced Prudential Standards regulations. She also served as legal centerpost on a major business integration consolidating the U.S. workforce under one legal entity and integrating business line management and operations across MUFG's legal entities in the Americas.

Maureen was previously a partner at a large international law firm, where she was a member of the Financial Institutions Corporate and Regulatory Group, Commercial Technology Group, and was Co-Chair and Co-Founder of the firm's Privacy and Security Group. Before joining the firm in 2003, Maureen was Assistant General Counsel in Bank of America's Legal Department, Regulatory and Corporate Services Group.

Maureen is well-established in the California and national banking and financial services industry. She is the immediate past Chair of the American Bar Association Banking Law Committee. She is a member of the Board of Directors of the Financial Women of San Francisco, currently serving as Co-Chair of the Programs Committee. She is former chair of the California Lawyers Association (State Bar) Financial Institutions Committee and the San Francisco Bank Attorneys Association. She organizes presentations and speaks regularly to financial and professional organizations.

She received her J.D. from University of California at Berkeley, School of Law, her Ph.D. and M.A. in Jurisprudence and Social Policy from University of California at Berkeley, and her A.B. (magna cum laude, Phi Beta Kappa) from Georgetown University.

Emily Yu
Seagate Technology LLC

Emily Yu is Lead Privacy Counsel at Seagate Technology, where she advises and assists the company with compliance on existing and emerging data protection regulatory requirements. Prior to joining Seagate, Emily worked at TrustArc as a Global Privacy Manager and assisted several Fortune 100 companies with privacy program management and compliance with a number of international standards and frameworks, including EU-US Privacy Shield, APEC CBPRs and GDPR validations. She is also one of the first graduates of SCU Law's Privacy Certificate program.

Polina Zvyagina

Airbnb Privacy Counsel

Polina is a Privacy Lawyer that specialized in Product work. She has worked at Apple, Uber and now Airbnb. She specializes in global scalable approaches to privacy by design, privacy training, product privacy and general privacy risk mitigation.

Prior to her legal career, she worked as an investigator at the NYC Civilian Complaint Review Board, where she investigated allegations of police misconduct.

1

California Consumer Privacy Act of 2018—Summary

Francoise Gilbert

Greenberg Traurig, LLP

Francoise Gilbert has practiced in the privacy and cybersecurity areas for almost 30 years. She advises organizations on the development and implementation of complex global compliance efforts, on cutting-edge privacy and cybersecurity issues surrounding emerging technologies such as the Internet of Things (IoT), artificial intelligence, smart cities and data analytics. She is the editor and lead author of the two volume treatise ***Global Privacy and Security Law***, www.globalprivacybook.com. She is admitted to practice law in the United States (California; Illinois) and in France (Paris Bar). She can be reached at fgilbert@globalprivacybook.com or +1-650-804-1235.

Table of Contents

1. OVERVIEW AND BACKGROUND 7
(A) Overview 7
(B) Legal and Constitutional Background 7
(C) Important Dates 7
2. ENTITIES SUBJECT TO CCPA 7
(A) Data Controllers Meeting a Specified Threshold 8
(B) Controlling or Controlled Entities 9
(C) Business Activities Excluded from the Scope of CCPA [Section 1798.145] 9
(D) Geographical Limitation 10
(E) Limitation of Applicability of Section 1798.110 to 1798.135 10
3. INDIVIDUALS PROTECTED BY CCPA 10
(A) California Residents 10
(B) Protection of Other Consumers; Freedom of Speech 12
(C) Protection of Freedom of Speech 12
4. INFORMATION PROTECTED BY CCPA 12
(A) Definition 12
(B) Not Just Electronic, but also Paper Records 14
(C) Exclusions from the Definition of Personal Information 14
(D) Information Outside the Scope of the CCPA 15
Medical Information 15
Credit Information 16
Financial Information 17
Driver's Information 17
(E) Deidentified and Aggregated Information 17
5. IMPORTANT DEFINITIONS 18
(A) Sale of Information 18
(B) Disclosure for a Business Purpose 19
6. CONSUMER'S RIGHT OF ACCESS TO INFORMATION 20
(A) Consumer's Right to Abbreviated Information [Section 1798.100] 20
(B) Consumer's Right to Detailed Information [Section 1798.110] ... 21
(C) Consumer's Right to Expanded Information about the Sale or Disclosure of Personal Information [Section 1798.115] 21
7. CONSUMER'S RIGHT OF ERASURE 22
8. CONSUMER'S RIGHT TO OPT-OUT OF OR OPT-IN TO THE SALE OF PERSONAL INFORMATION 22
(A) Right of Consumers Older than 16 22
(B) Right of Minors under 16 22
(C) Twelve-Month Window 23
(D) Right to Opt-Out Through Third Party Services 23

9. WAIVER AND WORK AROUND NOT ENFORCEABLE OR DISREGARDED 23
(A) Waiver Not Enforceable 23
(B) Workaround Disregarded 23
10. BUSINESSES' OBLIGATION TO RESPOND TO A REQUEST FOR INFORMATION 24
(A) Obligation to Provide Abbreviated Information [Section 1798.100] 24
Exception to the Obligation to Provide Information 24
(B) Businesses' Obligation to Provide Detailed Information [Section 1798.110] 24
Limit to Businesses' Obligations Regarding Right of Access 25
(C) Businesses' Obligations to Disclose What Personal Information They Have Sold or Disclosed [Section 1798.115] 26
(D) Extension of Time 27
(E) Notice of No Action 28
(F) Unfounded or Excessive Request 28
11. BUSINESSES' OBLIGATION REGARDING RIGHT OF ERASURE 28
(A) Exceptions to the Obligation to Delete Personal Information 28
(B) Exception for Research Purposes 29
12. BUSINESS OBLIGATIONS REGARDING OPT-OUT / OPT-IN RIGHT TO PROHIBIT THE OF SALE OF PERSONAL INFORMATION [SECTION 1798.120] 30
(A) Obligation to Inform Consumers of their Rights to Opt-out / Opt-in 31
(B) Obligation to Refrain from Selling Personal Information of Minors under 16 31
(C) Obligation to Refrain from Selling Personal Information without Proper Authorization 31
(D) 12-Month Window 32
(E) No Re-use of Personal Information 32
13. DISCRIMINATION BASED ON EXERCISE OF CONSUMER RIGHTS PROHIBITED; FINANCIAL INCENTIVES 32
(A) General Prohibition Against Discrimination Based on Exercise of Consumer Rights 32
(B) Exceptions to the Prohibition Against Discrimination 33
Different price or rates 33
Financial Incentives 33
(C) How to Enter into a Financial Incentive Program 33
14. CONTENT OF THE PRIVACY POLICY OR POLICIES 34
(A) Obligation to Provide Abbreviated Notice before Collecting Information [Section 1798.100(b)] 34
(B) Obligation to Provide Detailed Notice before Collecting Information [Section 1798.110(c)] 34

(C) Obligation to Provide Expanded Notice [Section 1798.115(c)] 35
(D) Where the Information Must be Provided 36
(E) Required Frequency of the Updates 36
15. OBLIGATION TO INFORM CONSUMERS OF THEIR RIGHTS 36
(A) Obligation to Inform about Practices 36
(B) Obligation to Inform Consumers about their Right of Erasure 37
(C) Obligation to Inform Consumers of their Rights to Opt-out / Opt-in 37
(D) Means of Implementing the Opt-Out 38
(E) Obligation to Inform Consumers of Financial Incentive Programs 38
16. SUBMISSION OF REQUESTS 38
(A) Obligation to Provide Consumers with Means for Submitting Requests 38
(B) What Constitutes a "Verifiable Consumer Request" 39
17. RESPONSE TO A CONSUMER'S REQUEST 40
(A) Timeline 40
(B) Verifiable Request 40
(C) Disclosure of Information Collected Over 12-Month Period 40
(D) Method for Disclosure 40
(E) Content of the Disclosure 41
(F) Delivery 41
(G) Not More Than Twice in a 12-Month Period 41
(H) Limitation on the Use of Information Collected to Verify the Identity of a Consumer 41
18. TRAINING OBLIGATIONS 42
(A) General Training Obligation 42
(B) Training with Respect to Opt-out of Sale of Personal Information 42
19. INTERACTION WITH SERVICE PROVIDERS AND THIRD PARTIES 42
(A) Service Providers 42
(B) Third Parties 43
(C) Exclusion from Liability for Third Parties' Acts 43
(D) Purchasers of Personal Information 44
20. ENFORCEMENT, INJUNCTIONS AND FINES [SECTION 1798.155] 44
(A) No Enforcement Actions Until July 1, 2020 44
(B) When a Violation Occurs 45
(C) Injunction and Fines 45
(d) Settlement Payment to be Made to Consumer Privacy Fund 45
21. CONSUMERS' PRIVATE RIGHT OF ACTION IN CASE OF SECURITY BREACH [SECTION 1798.150] 46
(A) Ability to File Civil Action for Specified Data Breaches 46

(B) Conditions for Filing Civil Action In Case of a Security Breach 46
Type of Information Protected 46
Type of Incident That May Trigger a Civil Action 48
Nature of the Civil Action 48
(C) Procedural Steps for an Action for Damages from a Security Breach [Section 1798.150(b)] 49
Action for Statutory Damages 49
Action Solely for Actual Pecuniary Damages 49
(D) Assessment of the Damages 50
22. DEVELOPMENT OF REGULATIONS AND PROCEDURES 50
(A) Development of Regulations 50
(B) Development of Rules and Procedures 50
23. ROLE OF THE STATE ATTORNEY GENERAL 52
(A) Provide Opinions [Section 1798.155(a)] 52
(B) Develop Regulations, Rules and Procedures 52
(C) Initiate Enforcement Actions 52
24. CONSUMER PRIVACY FUND 52
(A) Consumer Privacy Fund 52
(B) Fines to be Paid to Consumer Privacy Fund 53
25. CONFLICTS WITH OTHER LAWS 53

1. OVERVIEW AND BACKGROUND

(A) Overview

The California Consumer Privacy Act of 2018 (CCPA) is California's current attempt at regulating the collection and use of personal data.[1] Nicknamed a Mini GDPR, in reference to the European General Data Protection Regulation, Regulation (EU) 2016/679 ("GDPR"), the California law is more limited in scope than the lengthy, comprehensive GDPR. CCPA focuses on consumer's rights and aims at providing them with more detailed information about what information is collected, and what is done with it, as well as increased controls over the use of their personal information, especially the secondary uses that might not be obvious to individuals.

(B) Legal and Constitutional Background

According to its Section 1798.175, the CCPA is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, the California Online Privacy Protection Act (CalOPPA)[2] and the California statutes regarding the protection of Customer Records.[3]

(C) Important Dates

Under Section 1798.198(a), the CCPA becomes operative as of January 1, 2020, and under Section 1798.185(c), the California Attorney General may not bring an enforcement action under the CCPA until the final regulations issued under the CCPA are published or July 1, 2020, whichever is sooner.

2. ENTITIES SUBJECT TO CCPA

The CCPA applies to "businesses." The term "business" is defined in Section 1798.140(c) as either a for-profit entity that meets certain thresholds, or an entity that controls such for-profit entity.

1. Cal. Civ. Code §1798.100 *et seq.*
2. Cal. Bus. Prof. Code §§ 22575 *et seq.*
3. Cal. Civ. Code Title 1.81, commencing with Section 1798.80.

(A) Data Controllers Meeting a Specified Threshold

The first part of the definition focuses on businesses themselves. In that case the term "business" includes a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners. To be subject to the CPPA, these businesses must fulfill two criteria.

First, the business must:

- Collect consumers' personal information, or have a third part collect such information;[4]
- Alone, or jointly with others, determine the purposes and means of the processing[5] of consumers' personal information; and
- Do business in the State of California.

It is not clear to which extent not-for-profit entities are exempt from the scope of the CCPA. For example, there might be a difference in application between 501(c)(3) entities that are created for charitable purposes, and 501(c)(6), which perform as trade associations, and operate to advance the purposes of their members.

The second criteria relates to the entity's activities. To be a "business" subject to the law, the entity must satisfy one or more of three thresholds:[6]

- annual gross revenues in excess of twenty-five million dollars ($25,000,000) (to be adjusted from time to time); or
- alone or in combination, annually buys, sells, receives or shares for commercial purposes[7], the personal information of 50,000 or more consumers, households, or devices;[8] or

---

4. Under Cal. Civ. Code § 1798.140(e), the term "collect", or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.
5. The definition of processing is very broad. It includes "any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means". Cal. Civ. Code § 1798.140(q).
6. Cal. Civ. Code § 1798.140(c)(1).
7. "Commercial purposes" is defined in Section 1798.140(f) as to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

- derives 50 percent or more of its annual revenues from selling consumers' personal information.

Section 1798.185(a)(5) grants the Attorney General the task of adjusting the monetary threshold in Section 1798.140(c)(1)(A) to reflect any increase in the Consumer Price Index.

(B) Controlling or Controlled Entities

The other entities that are subject to the CCPA are entities that control or are controlled by a business, as defined above, and that share common branding with the business. "Common branding" is defined as a shared name, service mark, or trademark.[9]

For the purpose of the CCPA, "control" or "controlled" is defined as:[10]

- ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business;
- control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
- the power to exercise a controlling influence over the management of a company.

(C) Business Activities Excluded from the Scope of CCPA [Section 1798.145]

Cal. Civ. Code § 1798.145(a)(1)-(4) excludes from coverage of the CCPA activities of businesses that are required to:

- Comply with federal, state, or local laws.
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

"Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

8. Under Cal. Civ. Code § 1798.140(j), "device" is defined as any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device. Thus, information collected from or through IoT devices and intelligent vehicles would be included.
9. CCPA § 1798.140(c)(2).
10. CCPA § 1798.140(c)(2).

- Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
- Exercise or defend legal claims.

(D) Geographical Limitation

Cal. Civ. Code § 1798.145(a)(6) excludes from the scope of the CCPA any collection or sale of a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. A commercial conduct is deemed to take place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. However, storing personal information about a consumer when the consumer is in California - including storage on a device - and then collecting that personal information when the consumer and the stored personal information are outside of California remains prohibited under the CCPA.

(E) Limitation of Applicability of Section 1798.110 to 1798.135

Cal. Civ. Code § 1798.145(b) exempts a business from compliance with Sections 1798.110 to 1798.135, where such compliance would violate an evidentiary privilege under California law. In that case, the business would not be prevented from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

3. INDIVIDUALS PROTECTED BY CCPA

(A) California Residents

Protection under the CCPA extends only to individuals residing in California. Specifically, in Section 1798-140(g), a "consumer" is a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read

on September 1, 2017, however identified, including by any unique identifier.[11]

Section 17014 of the California Code of Regulation defines who is subject to taxation for California state tax purposes. At the simplest level, a California resident is (i) an individual who is in California for a purpose other than a temporary or transitory purpose or (ii) an individual who is domiciled in California and is outside the state for a temporary or transitory purpose.[12]

---

11. The term "unique identifier" or "unique personal identifier" is defined as a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody. Cal. Civ. Code § 1798.140(x).
12. Cal. Code of Regulations §17014 provides:
    (a) "Resident" includes:
        (1) Every individual who is in this state for other than a temporary or transitory purpose.
        (2) Every individual domiciled in this state who is outside the state for a temporary or transitory purpose.
    (b) Any individual (and spouse) who is domiciled in this state shall be considered outside this state for a temporary or transitory purpose while that individual:
        (1) Holds an elective office of the government of the United States, or
        (2) Is employed on the staff of an elective officer in the legislative branch of the government of the United States as described in paragraph (1), or
        (3) Holds an appointive office in the executive branch of the government of the United States (other than the armed forces of the United States or career appointees in the United States Foreign Service) if the appointment to that office was by the President of the United States and subject to confirmation by the Senate of the United States and whose tenure of office is at the pleasure of the President of the United States.
    (c) Any individual who is a resident of this state continues to be a resident even though temporarily absent from the state.
    (d) For any taxable year beginning on or after January 1, 1994, any individual domiciled in this state who is absent from the state for an uninterrupted period of at least 546 consecutive days under an employment-related contract shall be considered outside this state for other than a temporary or transitory purpose.
        (1) For purposes of this subdivision, returns to this state, totaling in the aggregate not more than 45 days during a taxable year, shall be disregarded.
        (2) This subdivision shall not apply to any individual, including any spouse described in paragraph (3), who has income from stocks, bonds, notes, or other intangible personal property in excess of two hundred thousand

(B) Protection of Other Consumers; Freedom of Speech

The rights granted to consumers under the CCPA are not absolute. Section 1798.145(j) provides that the CCPA states that the rights afforded to consumers and the obligations imposed on the business may not adversely affect the rights and freedoms of other consumers.

(C) Protection of Freedom of Speech

In addition, Section 1798.145(k) provides that the rights afforded to consumers and the obligations imposed on businesses do not apply to the extent that they infringe on the noncommercial activities of a person or entity described in Article I(2)(b) of the California Constitution. Article I(2)(b) of the California Constitution pertains to freedom of speech and generally protects publishers, editors, reporters, or other persons connected with or employed upon a newspaper, magazine, or other periodical publication.

4. INFORMATION PROTECTED BY CCPA

The definition of "personal information" (i.e., information protected under the CCPA, is very comprehensive, detailed and long. It is probably the longest definition of "personal information" or "personal data" anywhere in the world.

(A) Definition

Section 1798.140(o) defines "personal information" as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

---

dollars ($200,000) in any taxable year in which the employment-related contract is in effect. In the case of an individual who is married, this paragraph shall be applied to the income of each spouse separately.

(3) Any spouse who is absent from the state for an uninterrupted period of at least 546 consecutive days to accompany a spouse who, under this subdivision, is considered outside this state for other than a temporary or transitory purpose shall, for purposes of this subdivision, also be considered outside this state for other than a temporary or transitory purpose.

(4) This subdivision shall not apply to any individual if the principal purpose of the individual's absence from this state is to avoid any tax imposed by this part.

It should be noted that the "personal" information is attributed not only to an individual, but also to a household. Thus, for example, information about the whereabouts of a car could be deemed personal information of the family that owns the car.

Section 1798.140(o) goes on to provide a long list of specific examples of personal data. Specifically, the definition states that Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Any categories of personal information described in Section 1798.80(e).[13]
- Characteristics of protected classifications under California or federal law.
- Commercial information, including records of personal property, products or services[14] purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.[15]

---

13. Cal. Civ. Code § 1798.80 is part of California's statute regulating the disposal of customer records. Section 1798.80(e) defines "personal information" as "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Section 1798.80(e) also excludes from the definition of "personal information" information that is lawfully made available to the public when it is included in federal, state, or local government records.
14. Cal. Civ. Code § 1798.140(u) defines service(s) as work, labor, and services including services furnished in connection with the sale or repair of goods.
15. "Biometric information" is defined as an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited

- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.[16]
- Inferences[17] drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(B) Not Just Electronic, but also Paper Records

It should be noted that Section 1798.175 clarifies that the protections provided by CCPA are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Thus, the statute would also apply to information collected or retained on paper or other medium.

(C) Exclusions from the Definition of Personal Information

There are, however, limitations. CCPA §1798.140(o)(2) excludes "publicly available" information from the definition of personal information.

For the purposes of the CCPA, "publicly available" is defined as information that is lawfully made available from federal, state, or

---

to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information. Cal. Civ. Code § 1798.140(b).

16. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, 34 C.F.R. Part 99.
17. "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data. Cal. Civ. Code § 1798.140(m).

local government records, if any conditions associated with such information. However, biometric information collected by a business about a consumer without the consumer's knowledge is not deemed "publicly available" information.[18]

Further, the CCPA specifies that Information is not "publicly available" if it is used for a purpose that is not compatible with the purpose for which it is maintained and made available in the government records, or for which it is publicly maintained. "Publicly available" also does not include consumer information that is deidentified[19] or aggregate consumer information.[20]

(D) Information Outside the Scope of the CCPA

Section 1798.145(c) excludes from the scope of the CCPA personal information protected under other similar privacy laws. It should be noted that the CCPA contains exemptions for certain business activities and exemptions for certain categories of data. These include:

Medical Information

Section 1798.145(c)(1)(A) excludes from the scope of the CCPA "medical information" governed by the Confidentiality of Medical Information Act and "protected health information" that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued under the Health Insurance Portability and Accountability Act (HIPAA) and

18. CCPA § 1798.140(o)(2).
19. Under Section 1798.140(h), "deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; (2) has implemented business processes that specifically prohibit reidentification of the information; (3) has implemented business processes to prevent inadvertent release of deidentified information; (4) makes no attempt to reidentify the information.
20. "Aggregate consumer information" is defined as information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified. Cal. Civ. Code § 1798.140(a).

the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[21]

Section 1798.145(c)(1)(B) excludes from a scope of the CCPA a "provider of health care" governed by the Confidentiality of Medical Information Act or a covered entity governed by the privacy, security, and breach notification rules issued under HIPAA, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as specified in the Confidentiality of Medical Information Act, HIPAA or the HITECH Act.[22] It should be noted that this exclusion applies only to covered entities and does not apply to business associates.

Section 1798.145(c)(1)(B) excludes information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, or to the protection requirements of the United States Food and Drug Administration[23].

Credit Information

Under Section 1798.145(d), the CCPA does not apply to the sale of personal information to or from a consumer reporting agency when that information is provided in a consumer report or is used

---

21. Specifically, "medical information" governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) and "protected health information" that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104¬191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).
22. Specifically, a "provider of health care" governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).
23. Specifically, information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonization or pursuant to human subject protection requirements of the United States Food and Drug Administration.

to generate a consumer report within the scope of the US Fair Credit Reporting Act.[24]

Financial Information

Under Section 1798.145(e), the CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the:

- Federal Gramm-Leach-Bliley Act,[25] and implementing regulations, or
- California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code).

However, there is a carve out. The exclusion from the scope of the CCPA does not apply to those provisions that relate to consumer actions following a breach of security under Section 1798.150.[26]

Driver's Information

Finally, under Section 1798.145(f), the CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act.[27] There is a similar carve out as for the other exclusions described above. The exclusion from the scope of the CCPA does not apply to those provisions that relate to consumer actions following a breach of security under Section 1798.150.[28]

(E) Deidentified and Aggregated Information

The collection, use, retention, sale, or disclosure of consumer information that is deidentified or in the aggregate is also excluded from the scope of the CCPA.[29]

---

24. U.S. Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq*.
25. US Gramm-Leach-Bliley Act, Public Law 106-102.
26. These actions to claim damages for certain breaches of security affecting specified data are described below in section 21 "Consumer Private Right of Action for Security Breach".
27. US Driver's Privacy Protection Act of 1994, 18 U.S.C. §2721 *et seq*.
28. These actions to claim damages for certain breaches of security affecting specified data are described below in section 21 "Consumer Private Right of Action for Security Breach".
29. Cal. Civ. Code § 1798.145(a)(6).

Further, Section 1798.145(i) provides that CCPA may not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

5. IMPORTANT DEFINITIONS

(A) Sale of Information

What constitutes "selling" personal information is defined at length in Section 1798.140(t)(1). And Section 1798.140(t)(2) provides further clarification on what is not "selling."

Under Section 1798.140(t)(1), "sell," "selling," "sale," or "sold," means:

- selling,
- renting,
- releasing,
- disclosing,
- disseminating,
- making available,
- transferring, or
- communicating orally, in writing, or by electronic or other means,

a consumer's personal information to another business or a third party for monetary or other valuable consideration.

Section 1798.140(2) details the circumstances when a business is deemed not to be selling personal information. These are when:

> *(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.*
>
> *(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.*

(C) The business uses or shares with a service provider[30] personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act[31] ().

(B) Disclosure for a Business Purpose

What constitutes a "business purpose" is defined in Section 1798.140(d):

***"Business purpose"** means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another*

---

30. The term "service provider" includes any sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business. Cal. Civ. Code § 1798.140(w).
31. California Unfair and Deceptive Practices Act, Cal. Bus. Prof. Code, §§*17200 et seq.*

operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

6. CONSUMER'S RIGHT OF ACCESS TO INFORMATION

The CCPA contains several provisions giving a consumer the right to information. These provisions establish different levels of rights, which we categorize as "abbreviated", "detailed" and "expanded" for ease of differentiation.

(A) Consumer's Right to Abbreviated Information [Section 1798.100]

Cal. Civ. §1798.100(a) grants a consumer the right to request a business that collects the consumer's personal information to disclose

to that consumer the categories and specific pieces of personal information the business has collected.

(B) Consumer's Right to Detailed Information [Section 1798.110]

Section 1798.100 is supplemented by Section 1798.110. Section 1798.110 identifies in detail the information to which a consumer is entitled.

Specifically, Section 1798.110 grants a consumer the right to request a business that collects personal information about the consumer to disclose the following:

- The categories of personal information it has collected about that consumer
- The categories of sources from which the personal information is collected
- The business or commercial purpose for collecting or selling personal information
- The categories of third parties with whom the business shares personal information
- The specific pieces of personal information it has collected about that consumer

(C) Consumer's Right to Expanded Information about the Sale or Disclosure of Personal Information [Section 1798.115]

Section 1798.100 and 1798.110 are supplemented by Section 1798.115, which defines expanded obligations regarding the sale or disclosure of personal Information.

Section 1798.115(a) grants a consumer the right to request a business that sells the consumer's personal information, or discloses it for a business purpose, to provide the following information to that consumer:

- The categories of personal information that the business **collected** about the consumer.
- The categories of personal information that the business **sold** about the consumer

- The categories of third parties to whom the personal information was sold, listing the information by category or categories of personal information for each third party to whom the personal information was sold.
- The categories of personal information that the business **disclosed** about the consumer **for a business purpose.**

7. CONSUMER'S RIGHT OF ERASURE

The CCPA grants consumers a right to obtain the erasure or deletion of personal information collected. Under Section 1798.105(a) a consumer has the right to request that a business delete any personal information about the consumer that the business has collected from the consumer.

8. CONSUMER'S RIGHT TO OPT-OUT OF OR OPT-IN TO THE SALE OF PERSONAL INFORMATION

(A) Right of Consumers Older than 16

Section 1798.120(a) grants consumers the "right to opt-out". This right allows them, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. Section 1798.120(b) requires that they be informed of this right.

(B) Right of Minors under 16

Section 1798.120(c) creates special protections for minors under 16, referred to as the "right to opt-in". The statute distinguishes those who are between 13 and 16, from those who are under 13.

- The personal information of consumers between 13 and 16 years of age may not be sold unless the consumer has affirmatively authorized the sale of the consumer's personal information.
- The personal information of consumers who are less than 13 years of age may not be sold unless the consumer's parent or guardian has affirmatively authorized the sale of the consumer's personal information.

(C) Twelve-Month Window

It should be noted that Section 1798.135(a)(5) may provide a business with the ability to contact a consumer who has opted-out starting 12 months after being notified of the opt-out decision. Section 1798.135 (a)(5) requires the business to refrain from contacting the consumer for 12 months or more after receipt of an opt-out. Thus, upon expiration of the 12 month period, the business should be able to contact the consumer to request the consumer to reconsider the opt-out decision, and authorize the sale of the consumer's personal information.

(D) Right to Opt-Out Through Third Party Services

Section 1798.135(c) grants consumers the ability to authorize third parties to opt-out of the sale of the consumer's personal information on the consumer's behalf. It also requires businesses to comply with opt-out requests received from a person authorized by the consumer to act on the consumer's behalf. The details are to be specified in regulations to be adopted by the Attorney General.

9. WAIVER AND WORK AROUND NOT ENFORCEABLE OR DISREGARDED

(A) Waiver Not Enforceable

In addition, Under Cal. Civ. Code Section 1798.192, waivers are not enforceable. Any contractual provision that purports to waive or limit a consumer's rights under the CPPA, including, but not limited to, any right to a remedy or means of enforcement, will be deemed contrary to public policy and be void and unenforceable. However, the statute clarifies that Section 1798.192 should not be interpreted to prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

(B) Workaround Disregarded

Further, under Cal. Civ. Code Section 1798.190, workarounds intended to disguise a sale of personal information are prohibited. Specifically, Section 1798.190 specifies that if a series of steps or transactions are component parts of a single transaction intended to avoid

the restrictions of the CCPA, specifically, in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions.

10. BUSINESSES' OBLIGATION TO RESPOND TO A REQUEST FOR INFORMATION

(A) Obligation to Provide Abbreviated Information [Section 1798.100]

In response to a consumer's request under Cal. Civ. Code § 1798. 100(a), the business is required to provide that information upon receipt of a verifiable consumer request.

Section 1798.100(d) details the procedure to be followed. The business must:

- promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required.
- deliver the information by mail or electronically
- if providing the information electronically, it must provide the information in a portable format and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.

Further, the business is not required to provide personal information to a consumer more than twice in a 12-month period.[32]

Exception to the Obligation to Provide Information

Under Section 1798.100(e), a business is not required to retain any personal information that it collected for a single, one-time transaction, if the business does not sell or retain such information. It is also not required to reidentify or link information that is not maintained in a manner that would be considered personal information.

(B) Businesses' Obligation to Provide Detailed Information [Section 1798.110]

Section 1798.110 supplements Section 1798.100 to identify the type of information to be provided to a consumer in response to an access

32. See also CCPA § 1798.130(7).

request, and the means for responding. It also specifies limits to the businesses' obligations with respect to personal information.

Specifically, Section 110(b) requires that a business that collects personal information about a consumer disclose to the consumer:

- The categories of personal information it has collected about that consumer.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting or selling personal information.
- The categories of third parties with whom the business shares personal information.
- The specific pieces of personal information it has collected about that consumer.

The delivery of information must be made in accordance to the procedure specified in Section 1798.130(a)(3)(B).[33] The business must provide the information:

- Collected about the consumer in the preceding 12 months; and
- Organized by reference to the enumerated category or categories identified in the definition of "personal information" provided in Section 1798.140(o) that most closely describes the personal information collected.

In addition, Section 1798.130(b) reiterates the business's obligation to act upon receipt of a verifiable consumer request from the consumer. Section 1798.130(a)(3)(A) indicates that, to identify the consumer, the business must associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

Limit to Businesses' Obligations Regarding Right of Access

Section 1798.110(d) limits businesses' obligations regarding the handling of data access requests in two ways: Businesses are not required to retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of

33. Cal. Civ. Code §1798.110(b).

business, that information about the consumer is not retained. Further, businesses are not required to reidentify or link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(C) Businesses' Obligations to Disclose What Personal Information They Have Sold or Disclosed [Section 1798.115]

Section 1798.115(b) supplements the provisions of Section 1798.100(b) and 1798.110(b). Section 1798.115(b) requires that a business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, disclose, in respond to a consumer's request, upon receipt of a verifiable consumer request from the consumer:

- The categories of personal information that the business collected about the consumer;
- The categories of personal information that the business sold about the consumer;
- The categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and
- The categories of personal information that the business disclosed about the consumer for a business purpose.

The disclosure must be made in accordance with the requirements set forth in Section 1798.130(a)(4). Section 1798.130(a) outlines two sets of obligations: an obligation to properly identify the individual making the request, and an obligation regarding the content of the disclosure to be made.

Identification

Regarding identification, Section 1798.130(a)(4)(A) requires that the business first identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

Content of Disclosure

The obligations regarding the content of the disclosures, and the type of information provided are detailed in Sections 1798.130(a)(B) and 130(a)(C). The obligations include:

- The business must disclose, in two separate lists, information about the personal information that it has sold, and information about the personal information that it has disclosed for a business purpose.
- The list of categories required to be disclosed must follow the categories identified in the definition of personal information in Section 1798.140(o).
- Regarding the sale of personal information, the business must[34]
    - Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months;
    - Provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months;
- Regarding the disclosure of Personal Information for Business Purpose, the business must[35]
    - Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months;
    - Provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months.

(D) Extension of Time

While the general rule is that a business has 45 days to respond to a verified consumer request, Section 1798.145(g) allows for an extension of time. The time to respond may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business must inform the consumer of the need for such extension within 45 days of receipt of the request, and provide the reasons for the delay.[36]

34. Cal. Civ. Code § 1798.130(a)(4)(B).
35. Cal. Civ. Code § 1798.130(a)(4)(B).
36. Cal. Civ. Code § 1798.145(g)(1).

(E) Notice of No Action

If the business elects not to take action on the request of the consumer, it must inform the consumer, without delay and at the latest within the time period described above. The business must inform the consumer of the following:[37]

- The reasons for not taking action; and
- Any rights the consumer may have to appeal the decision to the business.

(F) Unfounded or Excessive Request

If requests from a consumer are manifestly unfounded or excessive – e.g., they are of a repetitive character - a business may:

- Charge a reasonable fee, that takes into account the administrative costs of providing the information or communication or taking the action requested, or
- Refuse to act on the request and notify the consumer of the reason for refusing the request.[38]

The business is responsible for demonstrating that the consumer's verified request is manifestly unfounded or excessive.[39]

11. BUSINESSES' OBLIGATION REGARDING RIGHT OF ERASURE

Cal. Civ. Code 1798.105(c) requires a business that receives a verifiable consumer request from a consumer to delete the consumer's personal information to

- Delete the consumer's personal information from its records; and
- Direct any service providers to delete the consumer's personal information from their records.

(A) Exceptions to the Obligation to Delete Personal Information

Section 1798.105(d) contains numerous exceptions to the obligation to delete personal information in response to a consumer's deletion

37. Cal. Civ. Code § 1798.145(g)(2).
38. Cal. Civ. Code § 1798.145(g)(3).
39. Cal. Civ. Code § 1798.145(g)(3).

request. A business or a service is required to comply with a request to delete a consumer's personal information if it is necessary for the business or service provider to maintain such information to:

- **Transactions**: Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or perform a contract between the business and the consumer.
- **Security**: Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- **Maintenance**: Debug to identify and repair errors that impair existing intended functionality.
- **Free speech**: Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
- **Investigations**: Comply with the California Electronic Communications Privacy Act.[40]
- **Research**: Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
- **Internal Use**: To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business, or use the personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.
- **Compliance:** Comply with a legal obligation.

(B) Exception for Research Purposes

The exception for research purposes is notable in that the definition section of the CCPA, in Section Cal. Civ. Code § 1798.140(s)

40. California Electronic Communications Privacy Act, Cal. Pen. Code, Part 2, Title 12, Chapter 3.6 (commencing with § 1546).

identifies in detail the criteria that an activity must meet in order to qualify as "research." Specifically,

> ***"Research"*** *means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:*
>
> *(1) Compatible with the business purpose for which the personal information was collected.*
>
> *(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.*
>
> *(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.*
>
> *(4) Subject to business processes that specifically prohibit reidentification of the information.*
>
> *(5) Made subject to business processes to prevent inadvertent release of deidentified information.*
>
> *(6) Protected from any reidentification attempts.*
>
> *(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.*
>
> *(8) Not be used for any commercial purpose.*
>
> *(9) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.*

12. BUSINESS OBLIGATIONS REGARDING OPT-OUT / OPT-IN RIGHT TO PROHIBIT THE OF SALE OF PERSONAL INFORMATION [SECTION 1798.120]

Section 1798.120 identifies three different obligations for businesses in connection with a consumer's ability to prohibit or prevent the sale of their personal information:

- An obligation to inform them of their right;

- An obligation to refrain from selling personal information of minors under 16 unless the business has received an opt-in, and
- An obligation to refrain from selling personal information of consumers aged 16 or older than 16 who have opted-out of the sale of their personal information.

(A) Obligation to Inform Consumers of their Rights to Opt-out / Opt-in

Section 1798.120(b) requires business that sell consumers' personal information to third parties shall provide notice to consumers that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information. See details in Section 8 [Consumers' Right to Opt-out / Opt-In to the Sale of Personal Information].

(B) Obligation to Refrain from Selling Personal Information of Minors under 16

Section 1798.120(c) prohibits a business from selling personal information of consumers under 16 if the business has actual knowledge that the consumer is less than 16 years of age, unless:

- in the case of consumers between 13 and 16 years of age, the consumer has affirmatively authorized, or "opted-in" to, the sale of the consumer's personal information.
- In the case of a consumer who is less than 13, if the consumer's parent or guardian, has affirmatively authorized, or opted-in to the sale of the consumer's personal information.

A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. Until regulations clarify when a business is deemed to have "willfully" disregarded a consumer's age, this prohibition is open for interpretation. For example it is not clear whether businesses should be required to follow guidance issued in similar circumstances by COPPA and its related regulations, or whether other criteria would apply.

(C) Obligation to Refrain from Selling Personal Information without Proper Authorization

Section 1798.120(d) specifically prohibits a business that has received direction from a consumer not to sell the consumer's personal

information (opt-out), or, in the case of a minor under 16 has not received consent to sell the minor consumer's personal information, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

Section 1798.120(d) makes a cross reference to Section 1798.135 (a)(4). However, that section does not provide further guidance. It merely states that the business must: "For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer".

(D) 12-Month Window

Section 1798.135(a)(5) states that when a consumer has opted-out of the sale of the consumer's personal information, the business must respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(E) No Re-use of Personal Information

Section 1798.135(6) prohibits businesses from using any personal information collected from the consumer in connection with the submission of the consumer's opt-out request. This information is to be used only for complying with the opt-out request.

13. DISCRIMINATION BASED ON EXERCISE OF CONSUMER RIGHTS PROHIBITED; FINANCIAL INCENTIVES

(A) General Prohibition Against Discrimination Based on Exercise of Consumer Rights

Section 1798.125(a)(1) prohibits businesses from discriminating against consumers who have exercised any of the consumer's rights provided by the CCPA, including, without limitation, by:

- Denying goods or services to the consumer.
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
- Providing a different level or quality of goods or services to the consumer.

- Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(B) Exceptions to the Prohibition Against Discrimination

The remainder of Section 1798.125 clarifies what is permitted or not, and how to implement financial incentives.

Different price or rates

Sections 1798.125(a)(2) and 1798.125(b)(1) allow businesses to charge different prices or rates, or provide different levels or quality of goods or services if that difference is "reasonably related to the value provided to the consumer by the consumer's data." The meaning of "value provided to the consumer by the consumer's data" is unclear at this moment. Upcoming regulations might provide needed guidance.

Financial Incentives

Section 1798.125(b)(1) allows businesses to offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. These financial incentive practices may not be unjust, unreasonable, coercive, or usurious in nature.[41]

(C) How to Enter into a Financial Incentive Program

A company that wishes to implement a financial incentive program must:[42]

- Notify consumers of the financial incentives, in accordance with the rules set forth in Section 1798.135;
- Clearly describe the material terms of the financial incentive program; and
- Obtain the consumer's prior opt-in consent pursuant to Section 1798.135;
- Allow the consumer to revoke his/her consent at any time.

41. Cal. Civ. Code § 1798.125(b)(4).
42. Cal. Civ. Code §§ 1798.125(b)(2) and (3).

14. CONTENT OF THE PRIVACY POLICY OR POLICIES

Throughout the CCPA, numerous provisions set forth requirements concerning the content of the Privacy Notice. In addition, Section 1798.130 (a)(5), reiterates or supplements these requirements.

These obligations of disclosure and transparency are detailed in other sections of the CCPA. Specifically they include the following:

(A) Obligation to Provide Abbreviated Notice before Collecting Information [Section 1798.100(b)]

Section 1798.100(b) requires a business that collects a consumer's personal information to inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used at or before the point of collection.

If the business intends to collect additional categories of personal information or use personal information collected for additional purposes, it is required to update its notice and provide a new notice to the consumer with notice consistent with this section.

(B) Obligation to Provide Detailed Notice before Collecting Information [Section 1798.110(c)]

Section 1798.110(c) supplements Section 1798.100(b) regarding businesses' obligations to provide information about their collection practices. Section 1798.110(c) lists the information to be provided:

- The categories of personal information collected
- The categories of sources from which the personal information is collected
- The business or commercial purpose for collecting or selling personal information
- The categories of third parties with whom the business shares personal information
- The specific pieces of personal information that the business collects.

In addition, Section 1798.110(c) cross-references Section 1798.130 (a)(5)(B), which specifies how that disclosure should be made. Section 1798.130(a)(5)(B) requires that:

- The statement describes the categories of personal information that the business has collected about consumers in the preceding 12 months
- The description be organized by reference to the enumerated category or categories of personal information that are listed in the definition of "personal information" provided in Section 1798. 140(o) that most closely describe the personal information collected.

(C) Obligation to Provide Expanded Notice [Section 1798.115(c)]

The obligations under Section 1798.100 and 1798.110 are supplemented and further expanded in Section 1798.115(c). The section requires businesses that sell consumers' personal information, or that discloses consumers' personal information for a business purpose, to disclose in their privacy notices:

Personal Information Sold

- The category or categories of consumers' personal information that the business has sold; or
- If the business has not sold consumers' personal information, state that the business has not sold consumers' personal information.

Personal Information Disclosed for Business Purpose

- The category or categories of consumers' personal information that the business has disclosed for a business purpose; or
- If the business has not disclosed the consumers' personal information for a business purpose, state that the business has not disclosed consumers' personal information for business purposes.

The nature of these disclosures is further detailed under Section 1798.130(a)(5)(C). Section 130(a)(5)(C) specifies how that disclosure should be made. It requires that:

- The disclosures be limited to the information sold or disclosed in the preceding 12 months
- The description be organized by reference to the enumerated category or categories of personal information that are listed

in the definition of "personal information" provided in Section 1798.140(o) that most closely describes the personal information collected.

(D) Where the Information Must be Provided

Section 1798.130(a)(5) requires businesses to provide information about their data handling practices:

- In their online privacy policy or policies; and
- In any California-specific description of consumers' privacy rights
- Or if the business does not maintain such policies, on its website.

(E) Required Frequency of the Updates

Section 1798.130(a)(5) also requires that the information be updated at least once every twelve months.[43]

15. OBLIGATION TO INFORM CONSUMERS OF THEIR RIGHTS

(A) Obligation to Inform about Practices

Section 1798.130(a)(5)(A) requires the Privacy Notice contain:

- a description of a consumer's rights pursuant to Sections 1798.110 [Right to know which information the business has collected], 1798.115 [Right to know which information has been sold or disclosed], and 1798.125 [Businesses' obligation not to discriminate]; and
- one or more designated methods for submitting requests for access to this information.[44]

43. Cal. Civ. Code § 1798.130(a)(5).
44. "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185. Cal. Civ. Code § 1798.140(i).

(B) Obligation to Inform Consumers about their Right of Erasure

Cal. Civ. Code 1798.105(b) requires a business that collects personal information about consumers to inform consumers that they have the right to request the deletion of their personal information. This information must be provided in accordance with Section 1798.130.

(C) Obligation to Inform Consumers of their Rights to Opt-out / Opt-in

Section 1798.120(b) requires businesses that sell consumers' personal information to third parties shall provide notice to consumers that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information. Section 1798.120 (b) is supplemented by Section 1798.135(a).

Cal. Civ. Code § 1798.135 defines the requirements relating to right to opt-out of (or opt-in to) the sale of personal information. Under Section 1798.135(a), a business that is required to comply must inform consumers about their rights regarding the sale of their personal information, and must provide the following information and capabilities in a form that is reasonably accessible to consumers:

- A clear and conspicuous link on the business's Internet homepage,[45] titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. The consumer must not be required to create an account in order to direct the business not to sell the consumer's personal information.
- A description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:
    - Its online privacy policy or policies if the business has an online privacy policy or policies.

45. Cal. Civ. Code § 1798.140(l) defines "home page" as the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by Section 1798.145(a), including, but not limited to, before downloading the application.

- Any California-specific description of consumers' privacy rights.

It is not clear whether the above disclosures are alternative or cumulative.

In addition, Section 1798.135 requires businesses to train their personnel as appropriate. See Section "Training Obligations," below.

(D) Means of Implementing the Opt-Out

Section 1798.135(b) provides additional guidance on developing means to provide users with their "opt-out right". Businesses may comply with the requirement to provide information regarding the opt-out rights by:

- providing a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and
- taking reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

There is not yet any guidance on what these "reasonable steps" would require.

(E) Obligation to Inform Consumers of Financial Incentive Programs

To the extent that a business wishes to implement a financial incentive program, it must notify consumers of the financial incentives, in accordance with the rules set forth in Section 1798.135 and clearly describe the material terms of the financial incentive program.[4647]

16. SUBMISSION OF REQUESTS

(A) Obligation to Provide Consumers with Means for Submitting Requests

Section 1798.130 requires businesses to make available to consumers means by which they can submit their requests regarding personal information when exercising their rights set forth in Sections 1798.100 [Right to Disclosure of Information Collected], 1798.105 [Right of

46. Cal. Civ. Code Sections 1798.125(b)(2) and (3).
47. See also Section 8 [Consumers Right to Opt-Out / Opt-In] above.

Erasure], 1798.110 [Right to Extended Disclosure], 1798.115 [Right Regarding Personal Information Sold or Disclosed], and 1798.125 [Financial Incentives].

Section 1798.130(a)(1) requires that the business make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 [Right to Extended Disclosure] and 1798.115 [Right Regarding Personal Information Sold or Disclosed], in a form that is reasonably accessible to consumers, including, at a minimum:

- a toll-free telephone number, and
- a website address, if the business maintains a website.

Ca. Civ. Code Section 1798.140(i) identifies other designated methods. Under Section 1798.140(i), "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(B) What Constitutes a "Verifiable Consumer Request"

Numerous sections of the CCPA require that the business respond to a consumer's request by first verifying the identity and legitimacy of the requesting person.[48] A request that has met these criteria is deemed a "verifiable consumer request".

Section 1798.140(y) defines a "verifiable consumer request" as a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify.

The definition then points to Regulations to be adopted by the Attorney General. A business is not obligated to provide information to the consumer in response to requests made under Sections 1798.110 and 1798.115 if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such

48. See, for example, Sections 1798.100; 1798.105; 1798.110; 1798.115; 1798.130.

consumer's behalf, using the guidance provided in the Attorney General's Regulations.

17. RESPONSE TO A CONSUMER'S REQUEST

Section 1798.130 identifies the methods for receiving consumers' requests regarding personal information; and the time to respond to these requests

(A) Timeline

The business must disclose and deliver the required information to the consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer.[49]

The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.[50]

(B) Verifiable Request

The business must promptly take the steps necessary to determine whether the request is a "verifiable consumer request".[51] The time to make such determination does not extend the 45 day time frame to deliver the information within 45 days of receipt of the consumer's request.

(C) Disclosure of Information Collected Over 12-Month Period

The disclosure must cover the 12-month period preceding receipt of the verifiable consumer request.[52]

(D) Method for Disclosure

The disclosure must be made in writing, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.[53]

---

49. Cal. Civ. Code § 1798.130(a)(2).
50. Cal. Civ. Code § 1798.130(a)(2).
51. See Section "What Constitutes a Verifiable Consumer Request" below.
52. Cal. Civ. Code § 1798.130(a)(2).
53. Cal. Civ. Code § 1798.130(a)(2).

(E) Content of the Disclosure

The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 must follow the definition of personal information in Section 1798.140(o).[54]

(F) Delivery

The disclosure must be delivered:[55]

- Through the consumer's account with the business, if the consumer maintains an account with the business;
- By mail or electronically at the consumer's option if the consumer does not maintain an account with the business.

The business may not require the consumer to create an account with the business in order to make a verifiable consumer request.

(G) Not More Than Twice in a 12-Month Period

Section 1798.130(b) provides that a business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(H) Limitation on the Use of Information Collected to Verify the Identity of a Consumer

Section 1798.130(7) clarifies that personal information collected from the consumer in connection with the business's verification of the consumer's request must be used solely for the purposes of verification. No further use of the information is permitted.

While this requirement makes sense, businesses should keep in mind that they must be able to show that they completed this process, and have a way to retain proof that they made the inquiry, reviewed the documentation, while ensuring that this information is kept in a secure manner, and separated from the remainder of the information.

It is not clear, as well, whether this information should be consulted if another inquiry is made allegedly on behalf of the same consumer, to compare the identity of the two requesting parties.

---

54. Cal. Civ. Code § 1798.130(c).
55. Cal. Civ. Code § 1798.130(a)(2).

18. TRAINING OBLIGATIONS

(A) General Training Obligation

Section 1798.130(a)(6) requires businesses to ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or its compliance with the CCPA are informed of all requirements in Sections 1798.110, 1798.115, 1798.125, and 1798.130, and how to direct consumers to exercise their rights under those sections.

(B) Training with Respect to Opt-out of Sale of Personal Information

Section 1798.135 requires businesses to train their personnel regarding the CCPA's provisions regarding the sale of personal information, which are set forth in Section 1798.120. Specifically, Section 1798.135 (a)(3) requires businesses to ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with its obligations are informed of all requirements in Section 1798.120 and 1798.135(a) and how to direct consumers to exercise their rights under those sections.

19. INTERACTION WITH SERVICE PROVIDERS AND THIRD PARTIES

While most of the CCPA applies to businesses and consumers, a small number of provisions address the interaction with third parties and service providers.

(A) Service Providers

Section 1798.140(v) defines a service provider as a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract. It also requires that the contract prohibit the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by the CCPA, including retaining, using, or

disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(B) Third Parties

The CCPA defines a third party as a person[56] other than the business that collects personal information from consumers and to whom the business discloses consumers' personal information for a business purpose pursuant to a written contract, provided that the contract:

- Prohibits the person receiving the personal information from:
  - Selling the personal information.
  - Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
  - Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
- Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(C) Exclusion from Liability for Third Parties' Acts

Section 1798.140(w)(1)(B) makes third parties that violate any of the restrictions set forth in the CCPA liable for the violations.

It also shields from liability under CCPA a business that discloses personal information to a third party subject to a written contract as described above, if the third party receiving the personal information uses it in violation of the restrictions set forth in the CCPA, provided that, at the time of disclosure, the business does not have actual knowledge, or reason to believe, that the third party intends to commit such a violation.

---

56. Note the use of "person" here. The definition is much broader than in the case of a "service provider" (see section above). Under CCPA, a "person" includes an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert. Cal. Civ. Code § 1798.140(n).

A similar provision is found in Section 1798.145(h), which states that a business that discloses personal information to a service provider is not liable if the service provider receiving the personal information uses it in violation of the restrictions set forth in the CCPA, if, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation.

Section 1798.145(h) also provides that a service provider is not liable for the obligations of a business for which it provides services as set forth in the CCPA.

(D) Purchasers of Personal Information

Section 1798.115(d) prohibits a third party that has purchased personal information from a business regulated under the CCPA from selling that personal information about a consumer unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

Section 115(d) does not specify which part of Section 1798.120 would govern. It is likely that the applicable provision might be Section 1798.120(b), which requires that a business that sells consumers' personal information to third parties to provide notice to consumers that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

The notice must be provided in accordance with Section 1798.135 (a).[57] Section 1798.135(a) details the requirements for notifying customers of their right to opt-out of the sale of their personal information. For details see Section "Right to Opt-Out", above.

20. ENFORCEMENT, INJUNCTIONS AND FINES [SECTION 1798.155]

(A) No Enforcement Actions Until July 1, 2020

Except for a limited private right of action in connection with security breaches,[58] all enforcement actions are within the purview of the California State Attorney General. However, Section 1798.185(b) limits this right. Enforcement actions may not be brought by the

57. Cal. Civ. Code § 1798.120(b).
58. See Section 21 [Consumers' Private Right of Section in Case of Security Breaches].

Attorney General until the earlier of (i) the publication of the final regulations or (ii) July 1, 2020.

(B) When a Violation Occurs

Section 1798.155(b) grants businesses 30 days after being notified[59] of an alleged non-compliance to cure the alleged violation. If, upon the expiration of the 30-day period the business has failed to cure the alleged violation, it is deemed to be in violation of the law. It may be subject to an injunction and fines.

(C) Injunction and Fines

Under Section 1798.155(b) any business, service provider, or other person[60] that violates the CCPA is exposed to:

- An injunction; and
- Liable for a civil penalty of:
  - Two thousand five hundred dollars ($2,500) for each violation; or
  - Seven thousand five hundred dollars ($7,500) for each ***intentional*** violation.

This penalty is to be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General; there is no private right action. Amendments are currently discussed that would allow for a private right of action for consumers.

(D) Settlement Payment to be Made to Consumer Privacy Fund

Any civil penalty assessed as set forth above and the proceeds of any settlement of an action brought as set forth above must be deposited in the Consumer Privacy Fund,[61] with the intent to fully

59. Presumably, this notification would be provided by the State Attorney General. It is not clear whether this notification could be made by or on behalf of a consumer.
60. Compare this sentence with the above sentence. The first line of Section 1798.155 (b) focuses on a "business". However, the second sentence continues with a reference to any "business, service provider or other person" rather than only "business".
61. Cal. Civ. Code § 1798.160. See also section "Consumer Privacy Fund," below.

offset any costs incurred by the state courts and the Attorney General in connection with this title.[62]

21. CONSUMERS' PRIVATE RIGHT OF ACTION IN CASE OF SECURITY BREACH [SECTION 1798.150]

(A) Ability to File Civil Action for Specified Data Breaches

Section 1798.150(a)(1) grants consumers the ability to institute a civil action to recover damages in event of a security breach that affects specific categories of personal information.

Section 1798.150(c) restates that the cause of action established by Section 1798.150 applies only to damages resulting from a breach of security affecting specified categories of data as detailed in Section 1798.150(a) and do not apply to violations of any other sections of the CCPA.

At the time of this writing, several bills are being prepared to enlarge the scope of the private right of action to the entire CCPA, rather than only to security breaches.

(B) Conditions for Filing Civil Action In Case of a Security Breach

Section 1798.150(a)(1) sets forth specific conditions and requirements for instituting a private civil action to recover damages in event of a security breach. Actions are limited to specific categories of personal information, and specific types of breaches of security. There are several limitations:

Type of Information Protected

The provision protected only non-encrypted or non-redacted personal information as defined in Cal. Civ. Section 1798.81.5[63]

62. Cal. Civ. Code § 1798.155(c).
63. The Personal Information protected under California's security breach disclosure law, Section 1798.81.5(d)(1)(A) includes:

- An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
  - Social security number.
  - Driver's license number or California identification card number.

The scope of the definition of "personal information" under Cal. Civ. Code Section 1798.81.5 is much narrower than that which is provided in the CCPA definition of "personal information under Cal. Civ. Code Section 1798.140(o).

Specifically, the "personal information" that is the subject of Cal. Civ. Code 1798.81.5 includes

- An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
    - Social security number.
    - Driver's license number or California identification card number.
    - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    - Medical information.
    - Health insurance information.
- A username or email address in combination with a password or security question and answer that would permit access to an online account.

When evaluating the effect of Section 1798.150(a), it important to keep in mind that the protection would be provided to only a small part of the personal information that is the subject of the CCPA, as described in Cal. Civ. Code 1798.140(o).

A civil action based on the private right of action granted by Section 1798.150(a)(1) in case a breach of security resulting from lack of reasonable security measures will apply to only those categories of personal information that California statutes have identified

---

    - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    - Medical information.
    - Health insurance information.
- A username or email address in combination with a password or security question and answer that would permit access to an online account.

Note that this range of information is much narrower than the information protected under the remainder of the CCPA.

as requiring reasonable security measures.[64] It is also the same type of personal information that requires disclosure of a breach of security under California's security breach disclosure laws,[65] and not the wider universe that is identified in Section 1798.140(o).

There are inconsistencies between the carve outs in Section 1798.81.5 and 1798.145 for medical information, financial information and other regulated information. The two sets of exceptions do not appear to overlap exactly. The passage of time may help understand whether the discrepancies are intentional, or may allow further amendments to ensure consistency between the two sets of exceptions.

Type of Incident That May Trigger a Civil Action

The incidents that might trigger instituting a civil action under Section 1798.150(a)(1) are limited to:[66]

- Unauthorized access and exfiltration, theft, or disclosure of personal information;
- That result from the violation of the business's duty to implement and maintain "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

Nature of the Civil Action

CCPA also limits the scope of relief that may be requested. Under Section 1798.150(a)(1)(A)-(C), the scope of the permitted civil actions described above is limited to civil actions for any of the following:

- To recover damages in an amount between one hundred dollars ($100) and seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater;

---

64. Cal. Civ. Code § 1798.81.5 identifies the type of information to be protected and requires businesses that own or license such information to implement reasonable security measures and to require their subcontractors by contract to maintain similar security measures to protect that information.
65. Cal. Civ. Code § 1798.82(a) (for businesses) and § 1798.29(e) (for State Agencies) require businesses and state agencies to report security breaches affecting categories of person information similar to those identified in Cal. Civ. Code § 1798.81.5.
66. Cal. Civ. Code § 1798.150(a)(1).

- Injunctive or declaratory relief; or
- Any other relief the court deems proper.

(C) Procedural Steps for an Action for Damages from a Security Breach [Section 1798.150(b)]

Section 1798.150(b) defines the required steps and path to follow an action for damages as described above. It distinguishes action for statutory damages from actions for actual pecuniary damages.

Action for Statutory Damages

- Before initiating any action against a business for statutory damages on an individual or class-wide basis, the consumer must provide a business 30 days' written notice identifying the specific provisions of the CCPA that the consumer alleges have been or are being violated.
- If a cure is possible, and if within the 30 day timeframe, the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, the consumer may not initiate an action for individual statutory damages or class-wide statutory damages initiated against the business.
- If the business continues to violate the CCPA in breach of the express written statement provided to the consumer as described above, then the consumer may initiate an action against the business to enforce the written statement, and may purse statutory damages for each breach of the express written statement, as well as other violation of the CCPA that postdates the written statement.

Action Solely for Actual Pecuniary Damages

If the action is limited to seeking violations for **actual pecuniary damages** suffered as a result of the alleged violations of this title, then the consumer may initiate the action without prior 30-day notice.

(D) Assessment of the Damages

Section 1798.150(a)(2) provides guidance to courts on how to assess the amount of statutory damages described in Section 1798.150 (a)(1)(A)-(C). It directs courts to consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to:

- The nature and seriousness of the misconduct;
- The number of violations;
- The persistence of the misconduct;
- The length of time over which the misconduct occurred;
- The willfulness of the defendant's misconduct and
- The defendant's assets, liabilities, and net worth.

22. DEVELOPMENT OF REGULATIONS AND PROCEDURES

(A) Development of Regulations

Cal. Civ. Code § 1798.185 requires that the California Attorney General solicit broad public participation and adopt regulations by July 1, 2020, in particular for the following purposes:

- Updating as needed additional categories of personal information in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.
- Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business.
- Establishing exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights.

(B) Development of Rules and Procedures

Section 1798.185 requires that the Attorney General establish rules and procedures for numerous aspects of the CCPA, within one

year of passage of the CCPA, and as needed thereafter. The issues to be addressed, as identified in Section 1798.185 include:

- To facilitate and govern the submission of opt-out requests to allow consumers to opt-out of the sale of personal information;
- To govern business compliance with a consumer's opt-out request;
- For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information;
- To ensure that the notices and information are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer;
- To offer financial incentives;
- To further the purposes of Sections 1798.110 and 1798.115 [Access to Information];
- To facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business;
- To determine that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request; and
- To provide a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity.

The Attorney General may adopt additional regulations as necessary to further the purposes of the CCPA.[67]

67. Cal. Civ. Code § 1798.185(b).

23. ROLE OF THE STATE ATTORNEY GENERAL

(A) Provide Opinions [Section 1798.155(a)]

CCPA contains an unusual provision concerning the role of the State Attorney General. Section 1798.155(a) grants any business or third party the ability to seek the opinion of the State Attorney General for guidance on how to comply with the provisions of the CCPA.

This provision is highly controversial, and the California State Attorney General has voiced concerns about the practical implementation of the provision given his limited staff and budget. A proposed amendment to the CCPA that would cancel or modify this provision is currently pending.

(B) Develop Regulations, Rules and Procedures

CCPA has assigned to the California Attorney General numerous obligations to develop regulations and procedures in specified areas. See Section 0 [Development of Regulations and Procedures].

(C) Initiate Enforcement Actions

CCPA grants the California Attorney General the right to enforce its provisions. See Section 20 [Enforcement, Injunctions and Fines].

24. CONSUMER PRIVACY FUND

(A) Consumer Privacy Fund

Section 1798.160 establishes the "Consumer Privacy Fund" and specifies that funds transferred to the Consumer Privacy Fund must be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with enforcement of the CCPA.[68] These funds may not be subject to appropriation or transfer by the Legislature for any other purpose, unless it is determined that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with its activities under the CCPA, in which case the Legislature may appropriate excess funds for other purposes.

68. Cal. Civ. Code § 1798.160(b).

(B) Fines to be Paid to Consumer Privacy Fund

Pursuant to Section 1798.155(b), any civil penalty assessed for a violation, and the proceeds of any settlement of an action brought under the CCPA are to be deposited in the Consumer Privacy Fund with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with these actions.

25. CONFLICTS WITH OTHER LAWS

Section 1798.175 addresses potential conflicts with other existing statutes. It specifies that, wherever possible, laws relating to consumers' personal information should be construed to harmonize with the provisions of the CCPA, and that if a conflict surfaces, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

In addition, Section 1798.180 provides that CCPA preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

Finally Section 1798.196 specifies that CCPA is intended to supplement federal and state law, if permissible, but will not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

NOTES

2

Lisa J. Sotto, Aaron P. Simpson and Brittany Bacon, Hunton Andrews Kurth LLP, 2018 Retail Industry Year in Review: California Consumer Privacy Act and Its Impact on Retailers

Submitted by:
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

HUNTON
ANDREWS KURTH

CALIFORNIA CONSUMER PRIVACY ACT AND ITS IMPACT ON RETAILERS



Lisa Sotto, Aaron Simpson and Brittany Bacon

Lisa is chair of the global privacy and cybersecurity practice and managing partner of the firm's New York office. Aaron and Brittany are partners in the global privacy and cybersecurity practice in the firm's New York office.

The California Consumer Privacy Act of 2018 (CCPA), signed by California Governor Jerry Brown on June 28, 2018, with a compliance deadline of January 1, 2020, signals a shift in the data privacy regime in the US. The CCPA was passed quickly by California lawmakers in an effort to remove a ballot initiative of the same name from the November 6, 2018, statewide ballot. The CCPA likely will require businesses, including retailers, to make significant changes to their data protection programs, if the business has consumers or employees who are California residents.

On September 23, 2018, Governor Brown signed into law SB-1121, which makes limited substantive and technical amendments to the CCPA. SB-1121 takes effect immediately and delays the California attorney general's (AG's) enforcement of the CCPA until six months after publication of the AG's implementing regulations, or July 1, 2020, whichever comes first.

Key provisions of the CCPA include:

- **Applicability.** The CCPA will apply to any for-profit business that: (1) "does business in the state of California"; (2) "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information"; and (3) satisfies one or more of the following thresholds: (a) has annual gross revenues in excess of $25 million; (b) alone or in combination, annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes, the personal information of 50,000 or more consumers, households or devices; or (c) derives 50 percent or more of its annual revenues from selling consumers' personal information (collectively, Businesses).
- **Definition of Consumer.** The CCPA defines "consumer" as a natural person who is a California resident.
- **Definition of Personal Information.** Personal information is defined broadly as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA's definition of personal information also contains a list of enumerated examples of personal information, which includes, among other data elements, name, postal or email address, Social Security number, government-issued identification number, biometric data, Internet activity information and geolocation data, as well as "inferences drawn from any of the information identified" in this definition.
- **Definition of Sale.** The CCPA broadly defines sale as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." The law provides several enumerated exceptions detailing activities that do not constitute a "sale" under the CCPA.

- **Privacy Policies.** The CCPA will require certain disclosures in businesses' online privacy notices, including a description of consumers' rights under the CCPA (e.g., the right to opt out of the sale of their personal information). Businesses must also disclose certain data practices from the preceding 12 months about the categories of personal information collected about consumers, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting or selling personal information and the categories of third parties with whom the business shares personal information. If the Business sells consumers' personal information or discloses it to third parties for a business purpose, the notice must also include lists of the categories of personal information sold or disclosed about consumers in the preceding 12 months.
- **Access Right.** Upon a verifiable request from a consumer, a business must disclose: (1) the categories and specific pieces of personal information the business has collected about that consumer; (2) the categories of sources from which the personal information is collected; (3) the business or commercial purposes for collecting or selling personal information; and (4) the categories of third parties with whom the business shares personal information. A Business that sells a consumer's personal information or discloses it for a business purpose must also disclose: (1) the categories of personal information that the business sold about the consumer; (2) the categories of third parties to whom the personal information was sold (by category of personal information for each third party to whom the personal information was sold); and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.
- **Deletion Right.** The CCPA will require a business, upon verifiable request from a consumer, to delete personal information about the consumer which the business has collected from the consumer and direct any service providers to delete the consumer's personal information. There are several enumerated exceptions to this requirement, two of which broadly state that compliance with a deletion request is not required when "it is necessary for the business or service provider to maintain the consumer's personal information" to: (1) "enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" or (2) "use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."
- **Opt-Out Right.** Businesses must provide a clear and conspicuous link on their website that says "Do Not Sell My Personal Information" and provide consumers a mechanism to opt out of the sale of their personal information, a decision which the Business must respect.
- **Specific Rules for Minors.** If a business has actual knowledge that a consumer is less than 16 years of age, the CCPA prohibits a business from selling that consumer's personal information unless: (1) the consumer is between 13-16 years of age and has affirmatively authorized the sale (i.e., they have opted in); or (2) the

consumer is less than 13 years of age and the consumer's parent or guardian has affirmatively authorized the sale.

- **Non-Discrimination and Financial Incentives.** Businesses cannot discriminate against consumers for exercising any of their rights under the CCPA. Businesses can, however, offer financial incentives for the collection, sale or deletion of personal information.
- **Enforcement.**
  - The CCPA is enforceable by the California AG and authorizes a civil penalty up to $2,500 for each violation or $7,500 for each intentional violation.
  - The CCPA provides a private right of action only in connection with certain "unauthorized access and exfiltration, theft, or disclosure" of a consumer's nonencrypted or nonredacted personal information, as defined in the state's breach notification law, if the business failed "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." The consumer may bring an action to recover damages up to $750 per incident or actual damages, whichever is greater.

Due to the CCPA's likely effect on the data protection programs of many businesses that have California consumers or employees, it is imperative that retailers develop a CCPA compliance strategy to determine the extent to which the law applies to them, assess their current CCPA compliance posture and conduct any necessary remediation activities.

NOTES

3

EU General Data Protection Regulation

Francoise Gilbert

Greenberg Traurig, LLP

Francoise Gilbert has practiced in the privacy and cybersecurity areas for almost 30 years. She advises organizations on the development and implementation of complex global compliance efforts, on cutting-edge privacy and cybersecurity issues surrounding emerging technologies such as the Internet of Things (IoT), artificial intelligence, smart cities and data analytics. She is the editor and lead author of the two volume treatise ***Global Privacy and Security Law***, www.globalprivacybook.com. She can be reached at fgilbert@globalprivacybook.com

§ 6A.01 INTRODUCTION

[A] Historical Background

At the beginning of the 2010's, the European Union embarked on a significant overhaul of its data protection regime. This overhaul touched upon both the protection of personal data that is collected and used in day-to-day business and commercial activities, and that of the information that is collected and used in connection with law enforcement activities. After an extensive study of the personal data collection and use practices and observation of the many changes in technologies since the early 1990's, two draft documents were released concurrently, by the European Commission, as a first step in building a new data protection regime for the twenty-first century.

These two documents were:

- A Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation or GDPR), intended to replace the 1995 Data Protection Directive; and
- A Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Directive), intended to replace the 2008 Data Protection Framework Decision.

These documents represented the most significant change to the personal data protection regime in the European Union in the past 25 years. The General Data Protection Regulation, which addresses the protection of personal data that is collected and used by businesses in day-to-day activities, is the most relevant to businesses located outside the European Union, or doing businesses with the European Union.

[B] Six-Year Development Process

The first draft of the GDPR and the Directive, prepared by the European Commission, were published in January 2012. They were then submitted to the European Parliament, which after making comments, additions, and deletions to the original EU Commission draft, adopted its version of the proposed documents in March 2014.

Thereafter, the Council of the European Union reviewed and prepared its comments and revisions of the proposed drafts in June 2015.

This concluded the initial phase of the drafting process where each of the three major EU organizations proposed their own versions of the GDPR and the Directive.

In the second phase of the drafting process, called the trilogue (i.e., dialogs and negotiations between the sponsors of the three drafts of the proposed GDPR and Directive) the EU Commission, the EU Parliament, and the Council of Ministers of the European Union met to agree on the details of a final draft of the documents. The outcome of these negotiations represented a compromise text agreeable to each of the three organizations.

[C] Final Draft and Vote

In mid-December 2015, the EU Presidency submitted a consolidated compromise text of the draft General Data Protection Regulation and draft Directive to the Permanent Representatives Committee as an outcome of the final trilogue.

The EU Parliament formally approved the final drafts of the EU General Data Protection Regulation and the Directive on April 14, 2016. The GDPR was published in the Official Journal of the European Union on May 28, 2016. However, there is a two-year transition period before the enforcement of the General Data Protection Regulation and the Directive. Consequently, enforcement of the GDPR and the Directive commenced, throughout the European Union on May 25, 2018.

§ 6A.02 GOAL OF THE GENERAL DATA PROTECTION REGULATION

The goal of the GDPR is to "reinforce the data protection rights of individuals, facilitate the free flow of personal data in the digital single market, and reduce administrative burden." This goal is to be interpreted within the framework of the fundamental belief that the protection of individuals in relation to the processing of personal data is a fundamental right. This belief permeates throughout the European Union and the European Economic Area, in activities of business and government institutions.

The European Union framework identifies the fundamental rights of individuals to include, among others:

- The right to respect private and family life, home, and communications;[1]

1. Charter of Fundamental Rights of the European Union, Art. 7.

- The right to the protection of personal data;[2]
- The freedom of thought, conscience and religion;[3]
- The freedom of expression and information;[4]
- The freedom to conduct a business;[5]
- The right to an effective remedy and to a fair trial;[6] and
- The right to cultural, religious, and linguistic diversity.[7]

The fundamental precept in the way in which the European Union approaches the protection of individuals with regard to the processing of their personal data is that anyone, whatever his nationality or residence, is entitled to the respect of his fundamental rights and freedoms, including the right to the protection of his personal data. The fundamental right to the protection of personal data is expressed in Article 8(1) of the Charter of Fundamental Rights of the European. Article 8 provides:

> *Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.*

However, this right to the protection of personal data is not an absolute right. The European Commission and the European Court of Justice have repeatedly stated that this right must be considered in relation to its function in society and must be balanced with other fundamental rights, in accordance with the principle of proportionality.

§ 6A.03 INTENT TO CREATE A UNIFORM FRAMEWORK

[A] Attempt to Create Uniformity

The GDPR drafters determined that in order to ensure a consistent level of protection for individuals throughout the EU and to prevent divergences hampering the free movement of data within the internal market, a Regulation was necessary to provide legal certainty and

2. Charter of Fundamental Rights of the European Union, Art. 8.
3. Charter of Fundamental Rights of the European Union, Art. 10.
4. Charter of Fundamental Rights of the European Union, Art. 11.
5. Charter of Fundamental Rights of the European Union, Art. 16.
6. Charter of Fundamental Rights of the European Union, Art. 47.
7. Charter of Fundamental Rights of the European Union, Art. 22.

transparency for businesses and the same level of legally enforceable rights for individuals in all Member States.

To this end, the EU Commission elected to draft a regulation rather than a directive after having determined that the nature of a directive had allowed Member States to choose the terms of their own interpretation of the 95/46/EC Directive in their own national laws. These different interpretations consequently resulted in the fragmented implementation of data protection across the EU, causing significant discrepancies among the Member States, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals.[8]

A regulation, however, could both impose the same obligations and responsibilities for data controllers and data processors; and ensure consistent monitoring of the processing of personal data as well as ensure equivalent sanctions in all Member States; and ensure effective cooperation by the supervisory authorities of different Member States.[9]

[B] Exceptions to Uniformity

Despite the decision that the EU new data protection framework should be defined in a Regulation that provided a uniform law with the same wording throughout the 31 EU and European Economic Area (EEA) Member States, the drafters recognized that there should be national differences in certain circumstances. There will continue to be numerous areas in which the Member States will continue to operate under their own rules.

Throughout the GDPR, numerous provisions give Member States the ability to supplement or supersede the GDPR with their own clauses or laws. For example, while the definition of "personal data" under the GDPR is limited to information concerning an identified or identifiable natural living persons—i.e., the Regulation will not protect the data of deceased persons—the GDPR allows Member States to provide for rules regarding the processing of data of deceased persons.[10]

Member States may modify the GDPR provisions that apply to the protection of children's personal data. Specifically, while the GDPR prohibits the processing of personal data of a child below the age of 16 years except with the consent or authorization of the holder of

8. GDPR, Preamble § 9.
9. GDPR, Preamble § 133.
10. GDPR, Preamble § 27.

parental responsibility,[11] it allows Member States to lower the age limit to 13 years.[12] Thus, it should be expected that the age limit for the prohibition against the collection and processing of children's personal data will vary from 13 to 16 years throughout the Member States.

Deviations are permitted, as well, in the area of the protection of special categories of personal data. The GDPR contains provisions limiting the processing of special categories of data, such as genetic data, biometric data, health data, religion, trade union membership, and several other categories of data. However, it also allows Member States to introduce their own conditions and limitations regarding the processing of genetic data, biometric data, or health data, even though these categories of data are already covered by the general provisions regarding special categories of data.[13]

In addition, it should be remembered that, in addition to the general data protection laws implementing Directive 95/46/EC, Member States have numerous sector specific laws in areas that contain more specific provisions. The GDPR allows Member States to specify their rules, including for the processing of sensitive data.[14] Further, the GDPR does not exclude or supersede national laws that define the circumstances of specific processing situations, such as to determine more precisely the conditions under which processing of personal data is lawful.[15]

[C] Carve Outs for Small and Medium-Sized Businesses

The GDPR contains derogations that exempt micro, small- and medium-sized enterprises from certain requirements. For example, there is an exemption from the record keeping requirement provisions for those organizations with fewer than 250 employees.

It also encourages the EU institutions and bodies, Member States and their respective supervisory authorities to take account of the specific needs of micro, small-, and medium-sized enterprises in the application of the GDPR.[16]

11. GDPR, Art. 8(1).
12. GDPR, Art. 8(1).
13. GDPR, Art. 9(4).
14. GDPR, Preamble § 8.
15. GDPR, Preamble § 8.
16. GDPR, Preamble § 13.

§ 6A.04 INTERPRETATION AND IMPLEMENTATION OF THE GDPR

[A] Initiatives of the Article 29 Working Party

The GDPR provided a two-year period for the implementation of the GDPR by Member States and covered entities to be completed before May 25, 2018, the enforcement date of the GDPR. To assist in the interpretation and implementation of the GDPR, between May 2016 and May 2018, the Article 29 Working Party published guidelines on GDPR-related matters. These guidelines have been endorsed by the European Data Protection Board (EDPB), the successor of the Article 29 Working Party.

[B] European Data Protection Board Guidelines

The Guidelines created by the Article 29 Working Party from May 2016 through May 2018 were endorsed by EDPB when the EDPB took over the responsibilities of the Article 29 Working Party on May 26, 2018.[17] The endorsed Guidelines can be found on the EDPB website.[18] They currently include:

- Guidelines on Consent under Regulation 2016/679, WP259 rev.01;
- Guidelines on Transparency under Regulation 2016/679, WP260 rev.01;
- Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679, WP251rev.01;
- Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01;
- Guidelines on the Right to Data Portability under Regulation 2016/679, WP242 rev.01;
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01;
- Guidelines on Data Protection Officers ("DPO"), WP243 rev.01;

17. https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.
18. Guidelines available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

- Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority, WP244 rev.01;
- Position Paper on the Derogations from the Obligation to Maintain Records of Processing Activities Pursuant to Article 30(5) GDPR;
- Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, WP 263 rev.01;
- Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264;
- Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265;
- Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01;
- Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01;
- Adequacy Referential, WP 254 rev.01; and
- Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253.

Both the Article 29 Working Party and the EDPB have noted that the Working Party previously published opinions and working papers with respect to issues arising under the 1995 EU Data Protection Directive and that pertain to matters that have not been significantly altered by the GDPR. They have indicated that these opinions and working papers remain valid and that companies should refer to these pre-existing opinions and working papers for questions arising under the GDPR that may have been addressed in these pre-existing documents. These documents have been archived and are available in the Article 29 Working Party archives.[19]

19. These archives are currently available at: https://ec.europa.eu/justice/article-29/documentation/index_en.htm.

[C] Initiatives of the Member States

The Member States have reacted in different ways to the adoption of the GDPR.

Some Member States, such as Germany, have opted to create a new law that replaces its current legal framework and that incorporates both the provisions of the GDPR and additional provisions.

Some Member States, such as Belgium and Estonia, have opted to make the GDPR their new personal data protection law and to focus on developing guidelines, guidance, and recommendations to assist in the interpretation of the GDPR. For example, Belgium has developed recommendations regarding the appointment of data protection officers and the use of data protection impact assessments.

The activities relating to the implementation of the GDPR at the country level are discussed in the chapters allocated to each EU or EEA country in this treatise.

§ 6A.05 THE PRINCIPAL PARTIES

[A] The People

[1] Data Subjects

A "data subject" is an identified or identifiable natural person. In this regard, an identifiable natural person is someone who can be identified, either directly or indirectly, in particular by reference to an identifier, such as name, an identification number, location data, and an online identifier or by one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.[20]

[B] The Leading Actors

[1] Data Controllers

A "data controller" is a natural or legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.[21] While the GDPR contains many of the data controller obligations that

20. GDPR, Art. 4(1).
21. GDPR, Art. 4(7).

were in the EU Directive 95/46/EC, it also provides for a number of new obligations, such as enhanced record keeping requirements. These obligations are discussed in further detail in this chapter.

[2] Data Processors

A "data processor" is a natural or legal person, public authority, agency, or another body, to which personal data are disclosed, where such individual or entity is a third party or not.[22] The GDPR assigns specific responsibilities for data processors; these are discussed in further detail in this chapter.

[3] Data Protection Officer

When a data controller or data processor conducts certain specified tasks, it is expected to appoint a data protection officer (DPO). The DPO may be a staff member of the data controller or data processor, or fulfill the tasks based on a service contract. Data protection officers have a unique status within an organization and are involved in all issues relating to the protection of personal data.[23] Among other things, their primary role is to advise the data controller or data processor of its obligations under the GDPR, and to monitor such compliance. The role, obligations, and powers of the DPOs are discussed in further detail in this chapter.

[C] The Government Entities

[1] Supervisory Authority

Each Member State is required to provide for one or more independent public authorities to be responsible for monitoring the application of the provisions of the GDPR, protecting the fundamental rights and freedoms of individuals in relation to the processing of their personal data and for facilitating the free flow of personal data within the EU.[24]

The primary role of a supervisory authority is to contribute to the consistent application of the GDPR throughout the EU. It is

22. GDPR, Art. 4(8).
23. The EDPB has endorsed Guidelines on Data Protection Officers (DPO's), WP243 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.
24. GDPR, Art. 51.

provided extensive powers. To ensure uniformity of application of the GDPR, the supervisory authorities are expected to cooperate with each other and the EU Commission within the framework defined by the GDPR.

[2] European Data Protection Board (EDPB)

The European Data Protection Board (EDPB) is the successor of the Article 29 Working Party.[25] It is composed of the head of one supervisory authority of each Member State, and of the European Data Protection Supervisor, or their respective representatives.[26] It is represented by its Chair.

[3] European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) is an independent supervisory authority whose primary role is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.[27] The EDPS participates in some meetings and decisions organized or made under the GDPR.

§ 6A.06 SUBJECT MATTER SCOPE

[A] Protection Limited to Living Natural Persons

The GDPR is limited to the protection of individuals or "natural persons."[28] It does not apply to the processing of data that pertain to legal persons, in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

While this approach is consistent with the 95/46/EC Directive on Data Protection, it should be noted that some of the existing EU/EEA Member States data protection laws, such as Lichtenstein, grant privacy right to corporate entities. It will be interesting to observe how the

25. The website of the EDPB is available at: https://edpb.europa.eu.
26. GDPR, Art. 68.
27. The nature, role and authority of the European Data Protection Supervisor are defined in Regulation (EC) No. 45/2001 (2001).
28. While the GDPR only applies to "natural persons," Member States may provide for rules regarding the processing of personal data of deceased persons. GDPR, Preamble § 27.

countries that offer data protection rights to corporate entities will react to the rules imposed by the GDPR.

[B] Type of Personal Data Protected

[1] Definition of Personal Data

The term "personal data" is defined as any information concerning an identified or identifiable natural living person. The GDPR will not protect the data of deceased persons. However, Member States may provide for rules regarding the processing of data of deceased persons.[29]

The full definition of personal data is longer and much more specific than under the Directive 95/46/EC. It provides:[30]

> "personal data" means any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data that has undergone pseudonymization and that could be attributed to a natural person by the use of additional information is also considered as information on an identifiable natural person.[31] However, anonymous information, i.e., information that does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable is outside the scope of the GDPR.

A person is deemed "identifiable" if the person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.[32] Whether a person is "identifiable" or can be identified will be decided by taking into account all the means reasonably likely to be used to identify the individual directly or indirectly, such as singling out either by the data controller or by another person.[33]

---

29. GDPR, Preamble § 27.
30. GDPR, Art. 4(1).
31. GDPR, Preamble § 26.
32. GDPR, Art. 4(1).
33. GDPR, Preamble § 26.

To ascertain whether means are "reasonable likely to be used to identify the individual," account will be taken of all objective factors, including the cost and amount of time required for such identification, as well as the nature of technology available at the time of the processing and further technological development.[34]

The GDPR Preamble makes it clear that individuals may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as Internet Protocol addresses, cookie identifiers, or other identifiers such as Radio Frequency Identification tags.[35] These identifiers may be combined with unique identifiers and other information received by servers, and may be used to create profiles of the individuals and identify them.[36]

[2] Sensitive Data

Several types of data receive special protection. Generally known as "sensitive data," these categories of data include: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data (when used to uniquely identify a natural person), data concerning health or a person's sex life or sexual orientation.[37] Compared to Directive 95/46/EC, the GDPR introduces two new categories of sensitive data: generic data and biometric data.

[3] Genetic Data

Genetic data was not covered specifically in the 95/46/EC Directive. The GDPR adds genetic data to the definition of the personal data. It defines the term "genetic data" as "personal data relating to the inherited or acquired genetic characteristics of a natural personal, which give unique information about the physiology or the health of that person and which result, in particular, from an analysis of a biological sample from the natural person in question."[38]

Under the GDPR, genetic data result from an analysis of a biological sample from the individual in question, in particular by

34. GDPR, Preamble § 26.
35. GDPR, Preamble § 30.
36. GDPR, Preamble § 30. See also Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
37. GDPR, Art. 9(1).
38. GDPR, Art. 4(13).

chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or from analysis of any other element enabling equivalent information to be obtained.[39]

[4] Personal Data of Children

Directive 95/46/EC did not address the protection of children's personal data. This is now changed with the GDPR. The GDPR acknowledges that children deserve specific protection of their personal data as they may be less aware of their rights in relation to the processing of personal data, and of the associated risks and consequences. This would include not only the collection of children's personal data when they use services offered directly to them, but also to the use of children's personal data for creating user profiles.

The GDPR prohibits the collection and processing of personal data of a child younger than 16 years old, except with the consent or authorization of the holder of parental responsibility over the child.[40] However, Member States are permitted to change this age limit once it is between 13 and 16 years.[41]

Further, data controllers are expected to make reasonable efforts to verify that the consent[42] is actually given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.[43] The GDPR also requires that when data processing concerns children, any information or communication be made in clear and plain language to ensure that children could easily understand what is being conveyed.[44]

[C] Extent of the Protection of Personal Data

The protection of individuals provided under the GDPR is intended to be technologically neutral and not dependent on any specific data processing techniques used.[45] Like the 95/46/EC Directive, the protection applies to processing of personal data both by automated

39. GDPR, Preamble § 34.
40. GDPR, Art. 8(1).
41. GDPR, Art. 8(1).
42. The EDPB Guidelines on Consent, "Guidelines on Consent under Regulation 2016/679 (WP 259 Rev. 01) are available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
43. GDPR, Art. 8(2).
44. GDPR, Preamble § 58.
45. GDPR, Preamble § 15.

means and by non-automated means—i.e., manually—if the data is contained or intended to be contained in a filing system.

The exclusions from coverage are similar to those set forth in Directive 95/46/EC. The following type of data or data files are outside the scope of the GDPR:[46]

- The processing of personal data by a natural person in the course of a purely personal or household activity such as correspondence, address books, social networking;
- Files and sets of files containing personal data that are not structured according to specific criteria;
- Personal data related to activities that fall outside the scope of European Union law, such as activities concerning national security;
- Personal data processed by Member States when carrying out activities related to the common foreign and security policy of the European Union; and
- The processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, such as the prevention of threats to public security.

§ 6A.07 TERRITORIAL SCOPE

[A] Covered Entities

[1] Entities Established in the European Union

The GDPR regulates the processing of personal data in the context of the activities of an establishment of a data controller or a data processor in the European Union, whether the processing takes place within the EU or not.[47]

The term "establishment" is defined as the effective and real exercise of activity through stable arrangements, such as a branch or a subsidiary, but the legal form of such arrangements is not the determining factor.[48]

46. GDPR, Art. 2.
47. GDPR, Art. 3(1).
48. GDPR, Preamble § 22.

[2] Entities Established Outside the European Union

In addition, the GDPR applies to data controllers and data processors not established in the EU if:

- The processing is related to the offering of goods or services to EU residents, whether or not the activity is connected to a payment or not; or
- The processing is related to the monitoring of the behavior of EU residents when their behavior takes places within the European Union.[49]

In the case of data controllers and data processors established outside the EU that have activities related to the offering of goods or services to EU residents, the determination whether the data controller or data processor is subject to the GDPR will take into account whether it is apparent that the data controller or data processor is envisaging the offering of services to data subjects in one or more EU Member States.[50] For example, the mere accessibility of a website in the EU, or the use of an email address or other contact details, or the use of a language generally used in a country other than where the data controller is established might be by itself insufficient to ascertain such an intention.[51]

However, additional factors may make it apparent that the data controller envisages offering goods or services to individuals residing in the EU.[52] Examples of additional factors include the use of a currency generally used in one or more EU Member States combined with the possibility of ordering goods and services in that other language, and/ or the mentioning of customers or users who are in the EU.

In the case of those data controllers and data processors outside the EU and whose processing is related to the monitoring of the behavior of EU residents when this behavior takes places within the European Union, the determination whether their activity qualifies as "monitoring," will be made by analyzing whether the information collected when tracking individuals is used for the

49. GDPR, Art. 3(2).
50. GDPR, Preamble § 23.
51. GDPR, Preamble § 23.
52. GDPR, Preamble § 23.

profiling,[53] in particular to take decisions concerning the individual or to analyze or predict the individual's personal preferences, behaviors and attitudes.[54]

[B] Main Establishment

[1] Main Establishment of a Controller

If a data controller is established in more than one Member State, the main establishment of a data controller located in the EU is normally the place of its central administration in the EU. However, if decisions on the purposes and means of processing of personal data are taken in another establishment of the data controller in the EU, and the latter establishment has power to have such decisions implemented, the establishment taking such decisions will be considered as the main establishment.[55]

The main establishment of a controller in the EU should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements.[56] It should not depend on whether the processing of personal data is actually carried out at that location.[57] The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment.

[2] Main Establishment of a Processor

In the case of a data processor with establishments in more than one Member State, the main establishment is the place where the processor has its central administration in the EU. If the data processor

53. The EDPB has published Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
54. GDPR, Preamble § 24.
55. GDPR, Art. (16)(a).
56. GDPR, Preamble § 36.
57. GDPR, Preamble § 36.

has no central administration in the EU, the place where the main processing activities take place in the EU will be the main establishment.[58]

[3] Main Establishment of a Group of Undertakings

Where the data processing is carried out by a group of undertakings, the main establishment of the controlling undertaking is that of the main establishment of the group of undertakings, unless where the purposes and means of processing are determined by another undertaking.[59]

[C] Controllers and Processors Established Outside the European Union

The GDPR applies to the processing of personal data of EU data subjects by a data controller or data processor not established in the Union, where the processing activities are related to (i) the offering of goods or services to EU data subjects, irrespective of whether the data subject is required to pay for these goods and services, to such in the Union; or (ii) the monitoring of EU data subjects' behavior to the extent it takes place within the EU.[60]

[1] Requirement to Appoint a Representative in the European Union

When a data controller or data processor meets the criteria above, it must designate in writing a representative in the EU, unless the processing is occasional and does not include, on a large scale, processing of special categories of data or data relating to criminal convictions and offences, and is unlikely to result in a risk for the rights and freedoms of individuals.[61]

[2] Obligations of the Representative of a Controller or Processors Established Outside the European Union

The representative must be established in one of the Member States where those data subjects whose personal data is processed in

58. GDPR, Art. 4(16)(b).
59. GDPR, Preamble § 36.
60. GDPR, Art. 3.
61. GDPR, Art. 27.

relation to the offering of goods or services to them, or whose behavior is monitored habitually reside.[62]

The primary role of the representative is to receive, in addition to, or in lieu of the data controller or the data processor, communications from the data protection supervisory authorities and data subjects on all issues related to the processing of personal data, and to ensuring compliance with the GDPR.[63]

The designation of a representative is without prejudice to any legal actions that could be initiated against the applicable foreign data controller or data processor.

§ 6A.08 GENERAL RULES FOR THE PROCESSING OF INFORMATION

[A] Overview

The GDPR sets forth six principles governing the processing of personal data:[64]

- ***Lawfulness, Fairness, Transparency***

  Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.[65]

- ***Purpose Limitation***

  Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes is not considered incompatible with the initial purposes.

- ***Data Minimization***

  Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

62. GDPR, Art. 27(3).
63. GDPR, Art. 27(4).
64. GDPR, Art. 5.
65. The European Data Protection Board (EDPB) has published guidelines on transparency: "Guidelines on Transparency under Regulation 2016/679 (WP 260 rev.01)," available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

- ***Accuracy***

  Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- ***Storage Limitation***

  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

  Personal data may be stored for longer periods to the extent that the data will be processed solely for archiving purposes in the public interest, or for scientific and historical research purposes or statistical purposes, subject to certain restriction, including the implementation of the appropriate technical and organizational measures.

- ***Integrity and Confidentiality***

  Personal data must be processed in a way that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

The principles are supplemented with a separate requirement for accountability. In addition to making the data controller responsible for compliance with the six principles, it also makes them responsible for being able to demonstrate compliance with these principles.

Most of these principles are similar to those that were the basis of the 95/46/EC Directive. However, there are some slight changes. The 95/46/EC Directive did not use the terms "transparency" or "accountability," which are concepts that are slightly more modern.

[B] Transparency

The concept of "transparency" requires that individuals are clearly informed that personal data concerning them is being collected, used, consulted, or processed and to what extent the data is processed or will be processed.

Individuals must be made aware of the risks, rules, safeguards, and rights in relation to the processing of personal data and how to exercise

his or her rights in relation to the processing. In particular, the specific purposes for which the data is processed should be explicit and legitimate and determined at the time of the collection of the data.

The principle of transparency also requires that any information addressed to the public or to data subjects be concise, easily accessible and easy to understand, that clear and plain language and, where appropriate, visualization be used.[66] This information could be provided in electronic form, for example through a website. The drafters of the GDPR were especially concerned about online advertising and its impact on processing of personal data, where the proliferation of actors and the technological complexity make it difficult for data subjects to understand that personal data about them is collected, by whom, and for what purpose.[67]

To assist in the interpretation and implementation of the GDPR provisions regarding transparency, the EDPB has endorsed the Guidelines on Transparency.[68]

[C] Accountability

The concept of accountability was also not present in Directive 95/46/EC. In Directive 95/46/EC, data controllers only had to "ensure that [the six principles] are complied with."[69] With the GDPR, there is a move away from notification requirements that data controllers previously had to adhere to and a move towards more accountability. The term "accountability" is located in numerous sections of the GDPR. It is expressed as part of the general "Principles Relating to Data Processing" (Article 5), in the form of a requirement that data controllers must demonstrate compliance with the applicable requirements laid down by the six principles.

[D] Processing of Special Categories of Data

[1] General Rule

Regarding the processing of sensitive data, the GDPR adopts the same reasoning as that of Directive 95/46/EC. It prohibits the

66. GDPR, Preamble § 58.
67. GDPR, Preamble § 58.
68. Guidelines on Transparency under Regulation 2016/679 (WP 260 rev.01), available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
69. Directive 95/46/EC, Art. 6(2).

processing of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a natural person or data concerning health or a person's sex life or sexual orientation.[70] It adds generic data and biometric data to the original list of sensitive data.

The concept of sensitive data is one where the U.S. and EU differ significantly. In the U.S., sensitive data is generally understood to be data that could, if misappropriated, lead to identity theft, such as driver's license information or credit card number, or to some form of stalking or harassment, such as might be the case with geolocation data. When it provides special treatment to certain categories of data that it deems sensitive, the EU focuses on personal data that is, by its nature, associated with fundamental rights and freedoms.

In the EU, the processing of the special categories of personal data is prohibited unless the processing fits within specified exceptions[71]

- The data subject has given explicit consent to the processing unless EU or Member State law provides that the prohibition may not be lifted by the data subject;[72]
- The processing is necessary for carrying out the obligations, and exercising specific rights of the data controller or of the data subject, in the field of employment and social security and social protection law in so far as it is authorized by EU or Member State law or by a collective agreement pursuant to law providing for appropriate safeguards for the fundamental rights and interests of the data subject;
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or non-profit-seeking body and relates solely to that

70. GDPR, Art. 9(1).
71. GDPR, Art. 9(2).
72. The EDPB Guidelines on Consent, "Guidelines on Consent under Regulation 2016/679 (WP 259 Rev. 01) are available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

body's members or to former members and that the data are not disclosed to others without the consent of the data subjects;

- The processing relates to personal data that are made public by the data subject;
- The processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law that must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable measures to safeguard the fundamental rights and interests of the data subject;
- The processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law, or pursuant to a contract with a health professional;
- The processing is necessary for reasons of public interest in the area of public health, subject to appropriate protection and professional secrecy;
- The processing is necessary for archiving purposes in the public interest, or scientific and historical research or statistical purposes based on EU or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

For example, data that fits within the group of special categories may only be processed for health-related purposes where necessary to achieve those purposes for the benefit of individuals and society as a whole, in particular in the context of the management of health or social care services.

[2] Special Rules

Member States are allowed to introduce further conditions, including limitations, with regard to the processing of genetic data,

biometric data, health data.[73] This is another area where there should be expected discrepancies among the Member States, especially given that the Member States often take significantly different approaches to the provision of healthcare and the payment for healthcare services

§ 6A.09 OBLIGATIONS OF DATA CONTROLLERS

The GDPR defines significant responsibilities and liabilities for any processing of personal data. It requires both data controllers and data processors to implement a wide variety of measures that take into account the nature, scope, context, and purposes of the processing and the risk for the rights and freedoms of individuals. In this regard, the GDPR goes well beyond the provisions of Directive 95/46/EC. Further, it requires data controllers—as well as data processors—to both implement appropriate and effective measures, and be able to demonstrate the effectiveness of these measures and their compliance with the GDPR.

[A] Obligation of Data Controllers

Data controllers are required to implement appropriate technical and organizational measures to ensure that the processing of personal data is performed in compliance with the GDPR.[74] They must review and update these measures where necessary.

These measures must take into account the nature, scope, context, and purposes of the processing, and the risks of varying likelihood and severity for the rights and freedoms of individuals.[75] These measures must include the implementation of appropriate data protection policies.[76]

Data controllers must be able to demonstrate their compliance.[77] To do so, they may adhere to approved codes of conduct or an approved certification mechanism.[78]

73. GDPR, Art. 9(44).
74. GDPR, Art. 24(1).
75. GDPR, Art. 25(1).
76. GDPR, Art. 25(1).
77. GDPR, Art. 25(1).
78. GDPR, Art. 25(3).

[B] Obligations of Data Controllers with Respect to the Rights of the Data Subjects

Data controllers have significant obligations to provide information related to how a data subject can exercise his rights of the data subjects. These obligations are addresed in this chapter.

[C] Data Protection by Design and by Default

Data controllers must implement measures to ensure data protection by design and by default. Data controllers can use an approved certification mechanism as an element to demonstrate compliance with these requirements.[79]

[1] Data Protection by Design

To ensure adequate data protection, a data controller is expected to implement appropriate technical and organizational measures both at the time of the determination of the means for processing and at the time of the processing itself.[80] He must integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

These measures must take into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing. They also must be adapted to face the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing. These measures may include, for example, pseudonymization. The GDPR points especially to the benefits of pseudonymization as a means to implement data protection principles, such as data minimization, in an effective manner.

The requirement also may be met by following the guidelines issued by an approved certification mechanism, and a certificate issued by such certificate mechanism may be used as an element to demonstrate compliance with the requirements.

[2] Data Protection by Default

Data controllers are also expected to implement appropriate technical and organizational measures for ensuring that, by default, the processing is limited to only that personal data necessary for a

79. GDPR, Art. 25(3).
80. GDPR, Art. 25.

specific purpose. This requirement applies to the amount of data collected, the extent of processing, the period of storage and the accessibility of the data. In particular, data protection by default measures must ensure that by default personal data is not made accessible to an indefinite number of individuals without the intervention of the data subject.[81]

The requirement also may be met by following the guidelines issued by an approved certification mechanism, and a certificate issued by such certificate mechanism may be used as an element to demonstrate compliance with the requirements.

[3] Suggested Measures

According to the GDPR, the measures to address data protection by design and by default requirements could consist, inter alia, of:[82]

- Minimizing the processing of personal data;
- Pseudonymizing personal data as soon as possible;
- Transparency with regard to the functions and processing of personal data;
- Enabling the data subject to monitor the data processing; and
- Enabling the data controller to create and improve security features.

Producers of products, services and applications, are encouraged when developing and designing products based on the processing of personal data or that process personal data, to fulfill their task to:[83]

- Take into account the right to data protection;
- Take into account due regard to the state of the art; and
- Make sure that data controllers and data processors are able to fulfill their data protection obligations.

81. GDPR, Art. 25(3).
82. GDPR, Preamble § 78.
83. GDPR, Preamble § 78.

[4] Joint Controllers

If several data controllers jointly determine the purposes and means of the processing of personal data, they are deemed "joint controllers." Data subjects may exercise their rights under the GDPR against each of the data controllers.[84]

Joint controllers must determine their respective responsibilities for compliance with their obligations under the GDPR, in particular in connection with their obligations to respond to requests for information, access, correction, deletion requests from data subjects as well as their respective obligations to provide information to data subjects. Joint controllers also must inform affected data subjects of their status as joint controllers.[85] They may designate a point of contact for data subjects.

[D] Data Controller's Obligations When Engaging a Data Processor

If a data controller intends to entrust a third party with the processing of personal data, the controller must use only data processors that provide sufficient guarantees to implement appropriate technical and organizational measures, so that the processing can meet the requirements of the GDPR, and ensure the protection of a data subject rights.[86]

These guarantees may include guarantees from the data processor in terms of expert knowledge, its reliability and resources, its ability to implement technical and organizational measures that will meet the requirements of the GDPR, including for the security of processing. Adherence by the data processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller.[87]

[E] Documentation of the Processing by a Data Controller

The 95/46/EC Directive required that data controllers notify their respective data protection supervisory authority of their data processing activities. Under the GDPR, this notification requirement is replaced by significant record keeping requirements that must be implemented by the data controllers themselves. Data controllers must keep records of

84. GDPR, Art. 26(3).
85. GDPR, Art. 26.
86. GDPR, Art. 28.
87. GDPR, Preamble § 81.

their processing activities.[88] Each data controller and, its representative, if any, is obliged to maintain a record of processing activities under its responsibility. The record must contain specified information:

- The name and contact details of the data controller, any joint controller, the data controller's representative and the data protection officer, if any;
- The purposes of the processing;
- The categories of data subjects;
- The categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries;
- If applicable, transfers of personal data to a third country (including the identification of the relevant third country);
- If applicable, documentation that establishes the legal basis for any cross-border transfers and the related safeguards;
- Where possible, the envisaged time limits for erasure of the different categories of data; and
- Where possible, a general description of the technical and organizational security measures used to protect the personal data in the data controller's custody.

The records must be in writing, including in an electronic form, and must be made available to the data protection supervisory authority, upon request.

Organizations with fewer than 250 employees are exempt from this record keeping requirement unless the processing (i) is likely to result in a risk for the rights and freedoms of data subject, (ii) is not occasional, (iii) includes special categories of data (e.g., health or trade union membership data), or (iv) is conducted on data relating to criminal convictions and offences.[89] The EDPB has endorsed a position paper on the Derogations from the Obligation to Maintain Records of Processing Activities Pursuant to Article 30(5) of the GDPR.[90]

88. GDPR, Art. 30.
89. GDPR, Art. 30(5).
90. Position Paper on GDPR Art. 30(5) available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045.

[F] Cooperation with the Supervisory Authority

A data controller and, if any, its representative, are required to cooperate, on request, with the data protection supervisory authority in the performance of its tasks.[91]

§ 6A.10 OBLIGATIONS OF DATA PROCESSORS

[A] Processing Under the Authority of the Controller

A data processor and any person acting under the authority of the data controller—or, in the case of a sub-processor, the sub-processor and any person acting under the authority of the primary processor—may not process personal data except on instructions from the data controller, or from the applicable primary processor, unless required to do so by EU or Member State law.[92]

[B] Written Contract Required

The processing of personal data by a data processor must be governed by a contract or other legal act, subject to EU or Member State law, binding the data processor to the data controller. The contract must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations, and rights of the data controller. In particular, the contract must require the data processor to:[93]

- Process the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to a third country, unless required to do so by EU or Member State law to which the data processor is subject;
- Ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Take all appropriate security measures required by the GDPR;
- Enlist another data processor only with the prior consent of the data controller and pursuant to a written contract with specified provisions;

91. GDPR, Art. 31.
92. GDPR, Art. 29.
93. GDPR, Art. 28(3).

- Assist the data controller by appropriate technical and organizational measures that take into account the nature of the processing in the fulfillment of the data controller's obligation to respond to data subject requests for access, erasure or correction of their personal data;
- Assist the data controller in ensuring compliance with its security obligations;
- At the data controller's request, delete or return all the personal data to it after the end of the data processing services, and delete existing copies unless EU or Member State law requires storage of the data;
- Make available to the data controller all information necessary to demonstrate compliance with the obligations under the GDPR, and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller; and
- Immediately inform the data controller if, in his opinion, an instruction by the data controller breaches any provision of the GDPR, or EU or Member State data protection provisions.

[C] Use of Sub-Processors

[1] Controller's Prior Consent Required

A data processor is prohibited from enlisting another data processor without the prior specific or general written consent of the controller. In the latter case, the data processor is required to always inform the data controller of any intended changes concerning the addition or replacement of other data processors, so that the data controller can object to these changes.[94]

If a data processor enlists another data processor for specific processing activities on behalf of the data controller, it must enter into a contract with the sub-processor that includes the same data protection obligations as those that are required in a contract between a data controller and a data processor. In particular, the contract must provide for the use of appropriate technical and organizational measures that are consistent with the requirements of the GDPR.[95]

94. GDPR, Art. 28(2).
95. GDPR, Art. 28(4).

If the sub-processor fails to fulfill its data protection obligations, the primary data processor remains fully liable to the data controller for the performance of that sub-processor's obligations.[96]

[2] Contract Between Data Controller and Data Processor

The processing by a processor must be governed by a binding contract that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the data controller. In addition, the contract must contain specified provisions. It must stipulate that the processor will:[97]

- Process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country, unless required to do so by applicable law to which the processor is subject; and in such a case, will inform the controller of that legal requirement before processing, unless prohibited from doing so by law;
- Ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Take all security measures required under the GDPR;
- Take the required precautions and obtain the required permissions when engaging another processor;
- Assist the controller by appropriate technical and organizational measures, in responding to data subjects' request in furtherance of the exercise of the rights granted to them under the GDPR;
- Assist the controller in ensuring compliance with the security measures and security breach disclosures required by the GDPR;[98]

96. GDPR, Art. 28(4).
97. GDPR, Art. 28(3).
98. The EDPB has published guidelines on procedures surrounding the occurrence of a breach of security affecting personal data. See Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

- At the controller's option, delete or return all personal data to the controller after the end of the engagement, and delete existing copies unless applicable law requires storage of such personal data;
- Make available to the controller all information necessary to demonstrate compliance with the obligations under the contract and the GDPR; and
- Allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

The contract between a data controller and a data processor may be based, in whole or in part, on standard contractual clauses.[99] The European Commission may lay down standard contractual clauses for use in this context.[100] In addition, a data protection supervisory authority may adopt standard contractual clauses, subject to compliance with the related consistency mechanism.[101]

[3] How to Demonstrate Compliance

A data processor may demonstrate its compliance with the requirements mandated by the GDPR by adhering to an approved code of conduct or an approved certification mechanism.[102]

[D] Documentation of the Processing by the Processor

Data processors' record keeping obligations are very similar to those of the data controllers. Each data processor and, if any, the data processor's representative is required to maintain a record of all categories of personal data processing activities that it carries out on behalf of a data controller. The record must contain:[103]

- The name and contact details of the data processor or sub-processors and of each data controller on behalf of which the data processor is acting, and, where applicable, the data controller's or the data processor's representative, and the data protection officer, if any;

99. GDPR, Art. 28(6).
100. GDPR, Art. 28(7).
101. GDPR, Art. 28(8).
102. GDPR, Art. 28(5).
103. GDPR, Art. 30.

- The categories of processing carried out on behalf of each data controller;
- If applicable, a description of the transfers of data to a third country, and in some instances, the documentation of appropriate safeguards; and
- Where possible, a description of the technical and organizational security measures being used.

Organizations with fewer than 250 employees are exempt from this record keeping requirement unless the processing being carried out (i) is likely to result in a risk for the rights and freedoms of data subject, (ii) is not occasional, (iii) includes special categories of data (e.g., health or trade union membership data) or (iv) is conducted on data relating to criminal convictions and offences.[104] The EDPB has endorsed a position paper on the Derogations from the Obligation to Maintain Records of Processing Activities Pursuant to Article 30(5) of the GDPR.[105]

§ 6A.11 CONSENT

[A] In General

The GDPR brings a new, more restrictive, definition of consent and new requirements for obtaining consent. Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[106]

Under the GDPR, consent will have to be given by a clear affirmative action by the data subject establishing a:[107]

- Freely given;
- Specific;

104. GDPR, Art. 30(5). See also Position Paper on GDPR Art. 30(5) available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045.
105. Position Paper on GDPR Art. 30(5) available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045.
106. GDPR, Art. 4(11).
107. The EDPB Guidelines on Consent, "Guidelines on Consent under Regulation 2016/679 (WP 259 Rev. 01) are available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

- Informed; and
- Unambiguous

Indication of the data subject's agreement to the processing of personal data relating to him or her.[108] This consent can be expressed through a written (including electronic), or oral statement.[109]

Several methods could be used for expressing this consent, these include the following:[110]

- Ticking a box when visiting an Internet website;
- Choosing technical settings for information society services; or
- A statement or conduct clearly indicating the specific context of the data subject's acceptance of the proposed processing.

However, the following will not be acceptable to demonstrate the consent of the data subject:

- Silence;
- Pre-ticked boxes; or
- Inactivity.

When the data processing has multiple purposes, consent would apply to all of the purposes disclosed in the notice, and would cover all processing activities carried out for the same purpose or purposes.

Further, Article 7 of the GDPR requires that a data controller must be able to demonstrate that a data subject has consented to the processing of his or her data where the processing is based on consent. A data subject has the right to withdraw his or her consent at any time; however, the withdrawal of consent will not affect the lawfulness of the processing already conducted prior to the withdrawal.[111]

[B] Consent as the Primary Basis for Lawful Processing

In order for processing to be lawful, personal data should be processed based on the consent of the person concerned or some other legitimate basis, laid down by law, either in the GDPR or in other EU

108. GDPR, Preamble § 32.
109. GDPR, Preamble § 32.
110. GDPR, Preamble § 32.
111. GDPR, Art. 7(3).

or Member State law as identified in the GDPR.[112] Other legitimate basis for processing include processing: (i) for the necessity of complying with a legal obligation to which the controller is subject; or (ii) necessary for the performance of a contract to which the data subject is party; or (iii) in order to take steps at the request of the data subject prior to entering into a contract.[113]

As discussed, where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and the extent to which consent is given.[114] The controller is expected to provide information in an intelligible and easily accessible form, using clear and plain language.[115]

For consent to be informed, the data subject must be aware at least of (i) the identity of the controller and (ii) the purposes of the processing for which the personal data is intended.[116] Further, consent will not be deemed freely given if the data subject has no genuine and free choice, and is unable to refuse or withdraw consent without detriment.[117]

The drafters of the GDPR were especially concerned about the circumstances where there is a clear imbalance between the data subject and the controller. Accordingly, consent is not presumed to be freely given if there is no possibility for separate consent to be given to different data processing operations, or if the performance of a contract, including the provision of a service, is made dependent on consent even though it is not necessary for such performance.[118]

[C] Processing Without Consent

[1] Compliance with Legal Obligation of the Controller

Where the processing is to be carried out without the consent of the data subject, and the legal basis for the lawfulness of the processing is (i) the need for compliance with a legal obligation to

112. The EDPB Guidelines on Consent, "Guidelines on Consent under Regulation 2016/679 (WP 259 Rev. 01) are available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
113. GDPR, Art. 6.
114. GDPR, Preamble § 42.
115. GDPR, Preamble § 42.
116. GDPR, Preamble § 42.
117. GDPR, Preamble § 42.
118. GDPR, Preamble § 43.

which the controller is subject or (ii) that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the GDPR stipulates that the processing have a basis in EU law, or in a Member State's national law.[119] That law should determine the purpose of processing, identify the type of controller to which it applies, the type of data that are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing.[120]

[2] Processing for the Legitimate Interest of the Controller

Like Directive 95/46/EC, the GDPR allows the processing of personal data for the legitimate interests pursued by the controller or a third party. However, in this case it is required to take into account the reasonable expectations of data subjects based on the relationship with the controller, and to balance the interest of the controller or third party against the interests or the fundamental rights and freedoms of the data subject, especially in the case of a child.[121]

Legitimate interest could exist when there is a relevant and appropriate relationship between the data subject and the data controller, for example, where the data subject is a client of the controller. The GDPR stresses that the existence of a legitimate interest requires careful assessment including whether a data subject can reasonably expect, at the time and in the context of the collection of the data, that the processing of his or her data for this purpose may take place.

The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data is processed in circumstances where a data subject does not reasonably expect further processing.[122]

The GDPR identifies a number of situations where the data controller may have a legitimate interest, For example:

- The processing of personal data strictly necessary for the purposes of preventing fraud constitutes a legitimate interest of the data controller concerned.[123]

119. GDPR, Art. 6(3).
120. GDPR, Art. 6(3).
121. GDPR, Preamble § 47.
122. GDPR, Preamble § 47.
123. GDPR, Preamble § 47.

- There might be situations where the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.[124]
- Data controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data.[125] However, in this case, the rules that govern the restrictions to the transfer of personal data to an entity located in a third country would still apply.
- The processing of data to the extent strictly necessary and proportionate for ensuring network and information security, such as preventing unlawful or malicious actions that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted data may also constitutes a legitimate interest of the data controller concerned.[126]

[D] Consent to the Use of Personal Data for Scientific Research

The GDPR recognizes that it is often not possible to identify fully the purpose of data processing for scientific research purposes at the time of data collection.[127] Therefore, data subjects are provided with the ability to give their consent to certain areas of scientific research.[128] Further, data subjects are granted the ability to consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

§ 6A.12 TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

[A] General Principles for Transfers

Any transfer of personal data to a third country for processing may only take place if the data controller and data processor comply with

124. GDPR, Preamble § 47.
125. GDPR, Preamble § 48.
126. GDPR, Preamble § 49.
127. GDPR, Preamble § 33.
128. The EDPB Guidelines on Consent, "Guidelines on Consent under Regulation 2016/679 (WP 259 Rev. 01) are available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

the appropriate safeguards laid down in the GDPR, including those conditions for onward transfers of personal data from the third country to another third country.[129]

[B] Transfers with an Adequacy Decision

A transfer of personal data to a third country may take place where the EU Commission has decided that the third country, or a territory or one or more specified sectors within that third country ensure an adequate level of protection. A transfer carried out under an adequacy decision by the EU Commission does not require any specific authorization.[130]

The GDPR requires the EU Commission to monitor developments in third countries that could affect the functioning of adequacy decisions on an on-going basis. The EU Commission may decide that a third country no longer ensures an adequate level of protection and, to the extent necessary, repeal, amend or suspend the adequacy decision.

Currently, several countries have succeeded in obtaining an EU Commission adequacy decision under Directive 95/46/EC. It is not clear at present whether these existing adequacy determinations will survive under the new GDPR. However, the GDPR provides that adequacy decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC will remain in force until amended, replaced, or repealed by an EU Commission decision.

[C] Transfers by Way of Appropriate Safeguards

Absent an adequacy decision, a data controller or data processor may transfer personal data to a third country only if the data controller or data processor has adduced appropriate safeguards, and if enforceable data subject rights and effective legal remedies for data subjects are available. These safeguards may or may not require specific authorization from a supervisory authority.

[D] Safeguards That Do Not Require an Authorization

The following safeguards may be used to provide a legal basis for a cross-border transfer, without requiring any specific authorization from a supervisory authority:[131]

129. GDPR, Art. 44.
130. GDPR, Art. 45.
131. GDPR, Art. 46(2).

- A legally binding and enforceable instrument between public authorities or bodies;
- Binding corporate rules;
- Standard data protection clauses adopted by the EU Commission;
- Standard data protection clauses adopted by a supervisory authority and approved by the EU Commission;
- An approved code of conduct with binding and enforceable commitments of the data controller or data processor in the third country to apply the appropriate safeguards, including those as regards data subjects' rights; or
- An approved certification mechanism together with binding and enforceable commitments of the data controller or data processor in the third country to apply the appropriate safeguards, including those as regards data subjects' rights.

[E] Safeguards That Do Require an Authorization

The following safeguards may be used to provide a legal basis for a cross-border transfer, only with a prior specific authorization from a supervisory authority:[132]

- Contractual clauses between the data controller or data processor and respective data controller, data processor or the recipient of the data in the third country; or
- Provisions to be inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights.

In these cases, the supervisory authority must apply the consistency mechanism referred to in Article 63.

At present, the status of pre-existing authorizations granted under Directive 95/46/EC is uncertain. The GDPR provides that the status of pre-existing authorizations granted by a Member State or by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. The status of decisions adopted by the EU Commission on the basis of Article 26(4) of Directive 95/46/EC also

132. GDPR, Art. 46(3).

remain in force until amended, replaced or repealed, if necessary, by an EU Commission decision.

[F] Transfers by Way of Binding Corporate Rules

Under the GDPR, all Member States are required to recognize binding corporate rules. The competent supervisory authority must approve binding corporate rules in accordance with the consistency mechanism if they:[133]

- Are legally binding and apply to and are enforced by every member of a group of entities or groups of enterprises engaged in a joint economic activity, including their employees;
- Expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
- Fulfill a number of stipulated requirements, which are detailed in the GDPR.

The GDPR stipulates the requirements for the content of the binding corporate rules. Binding corporate rules must contain at least the following:[134]

- The structure and contact details of the concerned group and of each of its members;
- The data transfers or set of data transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the third country or countries in question;
- Their legally binding nature, both internally and externally;
- The application of the general data protection principles, in particular purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- The rights of data subjects regarding the processing of their personal data and the means to exercise these rights, including the right not to

133. GDPR, Art. 47.
134. GDPR, Art. 47.

be subject to decisions based solely on automated processing, including profiling,[135] the right to lodge a complaint before the competent supervisory authority and before the competent courts of the respective Member State, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

- The acceptance by the data controller or data processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the EU. The data controller or the data processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage;
- How the information on the binding corporate rules is provided to the data subjects;
- The tasks of any data protection officer or any other person or entity in charge of monitoring training, complaint handling, and compliance with the binding corporate rules within the group;
- The complaint procedures;
- The mechanisms within the group for ensuring the verification of compliance with the binding corporate rules. These mechanisms must include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification must be communicated to the data protection officer (or equivalent) and to the board of the controlling undertaking or of the group of enterprises, and be available upon request to the competent supervisory authority;
- The mechanisms for reporting and recording changes to the binding corporate rules and reporting these changes to the supervisory authority;
- The cooperation mechanism with the supervisory authority to ensure compliance by any member of the group, in particular by making available to the supervisory authority the results of verifications of the audit;

135. The EDPB has published Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

- The mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group is subject in a third country and that are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- The appropriate data protection training provided to personnel having permanent or regular access to personal data.

The EDPB has endorsed a series of documents regarding the applications for approval of Binding Corporate Rules. These documents include:

- Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264;[136]
- Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265;[137]
- Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01;[138]
- Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01;[139] and
- Adequacy Referential, WP 254 rev.01.[140]

In addition, under GDPR Art. 47(3), the EU Commission may, in an implementing act, specify the format and procedures for the exchange of information between data controllers, data processors, and supervisory authorities for binding corporate rules. In the meantime, the EDPB has endorsed the Working Document Setting Forth a Co-Operation Procedure for Approval of "Binding Corporate Rules" for Controllers and Processors under the GDPR.[141]

136. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623850.
137. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848.
138. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.
139. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.
140. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
141. Working Document Setting Forth a Co-Operation Procedure for Approval of "Binding Corporate Rules" for Controllers and Processors under the GDPR available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056.

[G] Transfers or Disclosures Not Authorized by EU Law

The GDPR addresses the problem of the transfer of data in connection with litigation. It reiterates that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a data controller or data processor to transfer or disclose personal data may only be recognized or enforceable in any manner if it is based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer.[142] It is a reminder that special attention should be paid in particular to blocking statutes that prohibit certain transfers of data—personal or not—in connection with litigation.

[H] Derogations for Specific Situations

The GDPR retains the derogations previously available under Directive 95/46/EC. Specifically, in the absence of an adequacy decision, or appropriate safeguards, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization may take place only on condition that:[143]

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;[144]
- The transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken at the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise or defense of legal claims;

142. GDPR, Art. 48.
143. GDPR, Art. 49.
144. The EDPB Guidelines on Consent, "Guidelines on Consent under Regulation 2016/679 (WP 259 Rev. 01) are available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- The transfer is made from a register that, under EU or Member State law is intended to provide information to the public, and that is open to consultation by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in EU or Member State law for consultation are fulfilled in the particular case; or

Where a transfer cannot be based on an adequacy decision or appropriate safeguards, and none of the specified derogations is applicable, a transfer to a third country may take place under specified conditions. The transfer may occur only if it is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the data controller that are not overridden by the interests or rights and freedoms of the data subject, where the data controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data. The data controller must inform the competent supervisory authority and the concerned data subjects about the proposed transfer and the compelling legitimate interests pursued by the data controller.

[I] Guidelines on Crossborder Data Transfers

To assist in the interpretation and implementation of the GDPR provisions regarding crossborder data transfers, the Article 29 Working Party announced in October 2017 that it was preparing Guidelines on Cross Border Data Transfers. These Guidelines have not yet been published.

[J] International Cooperation for the Protection of Personal Data

The GDPR provides the structure for international cooperation with other organizations for the protection of personal data.[145] It requires the EU Commission and supervisory authorities to take appropriate steps to develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal

145. GDPR, Art. 50.

data; and provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms. It also requires them to engage relevant stakeholders in discussions and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; and promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

§ 6A.13 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. The drafters of the GDPR determined that this obligation produced administrative and financial burdens, but did not necessarily contribute to improving the protection of personal data in all cases.

Accordingly, they opted to abolish this notification requirement and to replace it by procedures and mechanisms that cover those processing activities likely to result in a high risk to the rights and freedoms of individuals by virtue of their nature, scope, context, and purposes. For example, this procedure might apply in cases that involve the use of new technologies or where such an assessment becomes necessary in the light of the time that has elapsed since the initial processing.

To supplement the detailed provisions of GDPR Article 35, the EDPB has endorsed Guidelines on Data Protection Impact Assessment (DPIA) and Determining Where Processing is "Likely to Result in a High Risk" for the purpose of Regulation 2016/279, WP 248 Rev. 01.[146]

[A] Data Protection Impact Assessment (DPIA)

[1] When a Data Protection Impact Assessment Is Required

Where a type of processing is likely to result in a high risk for the rights and freedoms of individuals, a data controller is required to carry out an assessment of the impact of the envisaged processing

146. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

operations on the protection of personal data before commencing the processing (i.e., a data protection impact assessment, or DPIA). This is the case in particular when the processing requires or relies on the use of new technologies. The evaluation should take into account the nature, scope, context, and purposes of the processing.[147] A single assessment may address a set of similar processing operations that present similar high risks.

If the data controller has appointed a data protection officer, it must seek the advice of the data protection officer when carrying out a DPIA.[148]

The DPIA guidelines indicate that, when it is not clear whether a DPIA is required, it is recommended that a DPIA be carried out nonetheless because a DPIA is useful tool to help controllers comply with data protection laws.[149]

[2] Cases That Require a Data Protection Impact Assessment

There are a number of situations where a DPIA must be conducted. Specifically, a DPIA must be completed at least in the following cases:[150]

- The systematic and extensive evaluation of personal aspects relating to natural persons is planned, and that evaluation is based on automated processing, including profiling,[151] and on which decisions that produce legal effects concerning the individual or similarly significantly affect individuals are based;
- The processing on a large scale of special categories of data (e.g., health data, data concerning race or ethnic origin), or of data relating to criminal convictions and offences is contemplated; or

147. GDPR, Art. 35(1).
148. GDPR, Art. 35(2).
149. See page 8, Guidelines on Data Protection Impact Assessments (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2017/679, WP 248 Rev. 01.
150. GDPR, Art. 35(3).
151. The EDPB has published Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

- The systematic monitoring of a publicly accessible area on a large scale is planned.

Each Member State's supervisory authority has the authority to establish and make public a list of the kind of processing operations that require a DPIA. A supervisory authority also may establish and make public a list of the type of processing operations for which no DPIA is required. In both cases, the supervisory authority must communicate those lists to the European Data Protection Board.[152]

The guidelines concerning DPIA list a number of cases where the preparation of the DPIA would be required, including, for example, the following:[153]

- Evaluation or scoring, profiling, and predicting from aspects concerning the data subject's performance at work; economic situation; health; personal preferences or interests; reliability of behavior; location or movement;
- Automated decision making with legal or similar effect, e.g., leading to exclusion or discrimination;
- Systematic monitoring of a publicly accessible area;
- Collection and processing of sensitive data; information collected for purely personal purposes and stored in the cloud;
- Data processing on a large scale (number of data subjects concerned, volume of data, duration, geographic extent of the processing);
- Data sets that have been matched or combined;
- Data concerning vulnerable data subjects;
- Innovative uses of technology;
- Data transfers outside the EU; and
- When the processing prevents data subject from exercising a right or using a service.

152. GDPR, Art. 35(5).
153. See pages 10-11, Guidelines on Data Protection Impact Assessments (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2017/679, WP 248 Rev. 01.

[3] Process for Conducting a DPIA

The DPIA guidelines identify the process to be followed for conducting a DPIA.

- The DPIA should be conducted prior to the processing (same as data protection by design or by default);
- The data controller will always be responsible for the conduct and content of the DPIA and the conclusions made, even if a third party conducts it;
- When a data controller has a data protection officer (DPO), it must seek advice of the DPO, and document it;
- The data controller must seek the views of data subjects or their representatives, where appropriate;
- The DPIA must define and document other specific roles and responsibilities depending on internal policy, processes and rules;
- The DPIA should be published in whole or in part, but this is not a legal requirement; and
- The DPIA must be communicated to the supervisory authority in case of prior consultation.

[4] Content of Assessment

The DPIA must contain at least the following:[154]

- A systematic description of the proposed processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the rights and freedoms of data subjects; and
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data, and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

154. GDPR, Art. 35(7).

Compliance with approved codes of conduct by the relevant data controllers or data processors is also taken into account in assessing the impact of the processing, in particular for the purposes of a DPIA.

[B] Consultation with Data Subject

Where appropriate and as part of the impact assessment, the data controller may seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.[155] It remains to be seen how this requirement will be implemented because most developments of new applications are conducted in secret, and it does not seem practicable to consult the public unless strong confidentiality agreements are in place.

[C] Prior Consultation of Supervisory Authority

[1] When Prior Consultation Is Required

While the GDPR phases out the requirements for prior notice and prior authorization, it introduces the concept of "prior consultation" for the most extreme data processing situations. A data controller is required to consult the supervisory authority before processing personal data if a DPIA indicates that the processing would result in a high risk unless the data controller takes specific measures to mitigate the risk.[156]

The DPIA guidelines expand the grounds for prior consultation with the supervisory authority and explain the process to be followed. The Guidelines clarify that the data controller is responsible for assessing the risks to the rights and freedoms of the data subjects and identifying the measures necessary to reduce those risks. If the risks cannot be sufficiently addressed, the data controller must consult the supervisory authority.

This would occur, for example in the following situations:

- The data subjects may encounter significant or irreversible consequences that they may not overcome;
- When it seems obvious that the risk will occur;

155. GDPR, Art. 35(9).
156. GDPR, Art. 36(1).

- When the data controller cannot find sufficient measures to address the risk; or
- When Member State law requires consultation with, or prior authorization from the supervisory authority.

If the supervisory authority determines that the intended processing would not comply with the GDPR, in particular where the data controller has insufficiently identified or mitigated the risk, the supervisory authority may intervene within eight weeks following the request for consultation and give advice to the data controller. This period may be extended for a further six weeks, taking into account the complexity of the intended processing.

[2] Formalities for Prior Consultation

When consulting the supervisory authority, the controller must provide the following information:

- Where applicable, the respective responsibilities of data controller, joint controllers, and data processors involved in the processing, in particular for processing within a group of undertakings;
- The purposes and means of the intended processing;
- The measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the GDPR;
- Where applicable, the contact details of the DPO;
- The DPIA; and
- Any other information requested by the supervisory authority.

[D] Additional Requirements Under Member State Laws

Member States are allowed to adopt national laws that may require data controllers to consult with, and obtain prior authorization from, the supervisory authority in the case of processing for the performance of a task carried out by the data controller in the public interest, such as in connection with social protection and public health.[157]

157. GDPR, Art. 36(5).

[E] Fines

The DPIA guidelines also clarify the conditions under which an administrative fine might be assessed against a company that does not meet its obligations to conduct a DPIA. According to the guidelines, a fine of up to EUR 10 million or up to 2% global revenue might be assessed in case of:

- Failure to carry out a DPIA when it is required;
- Carrying out a DPIA in an incorrect way and
- Failure to consult with competent supervisory authority.

§ 6A.14 SPECIAL CATEGORIES OF PROCESSING

[A] Processing in the Context of Employment

Member States are granted significant freedoms to supplement the provisions of the GDPR in the context of employment. They may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in the case of the processing of employees' personal data in the employment context.[158]

This leeway is provided in particular for the use of personal data in the context, amongst other measures, of recruitment, the performance of an employment contract, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, and health and safety at work.

If a Member State elects to implement additional rules, the rules must include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights. Special attention must be given to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity, and monitoring systems at the work place.

Each Member State is required to notify the EU Commission of those provisions of its law that it adopts, pursuant to Article 88, by May 25, 2018. Thereafter each Member State will have to notify any subsequent amendment.

158. GDPR, Art. 88.

[B] Freedom of Expression and Information

Member States are required to adopt laws that reconcile the right to the protection of personal data pursuant to the GDPR with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.[159]

For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States must provide for exemptions or derogations from provisions of the GDPR. These exemptions or derogations will apply to those provisions regarding the general data processing principles, the rights of data subjects, the obligations of data controllers and data processors, the transfer of personal data across borders, the role and obligations of supervisory authorities, the rules of cooperation and consistency if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.[160]

Each Member State is required to notify to the EU Commission of the provisions of its law that it has adopted pursuant to Article 85, as well as any subsequent amendment law or amendment affecting them.

[C] National Identification Number

Member States are allowed to determine the specific conditions for the processing of a national identification number or any other identifier of general application.[161] National identification numbers or any other identifier of general application may be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to the GDPR.

[D] Public Access to Official Documents

Disclosure of personal data is permitted in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest.[162] The disclosure must be performed by the relevant authority or body in accordance with the EU or a Member State law to which the public authority or

159. GDPR, Art. 85.
160. GDPR, Art. 85(2).
161. GDPR, Art. 87.
162. GDPR, Art. 86.

body is subject in order to reconcile public access to official documents with the right to the protection of personal data.

[E] Processing for Archiving Purposes in the Public Interest

When data is processed for archiving purposes in the public interest, the GDPR requires that it be protected with appropriate safeguards, consistent with the provisions of the GDPR, in order to safeguard the rights and freedoms of the data subjects. Those safeguards must include the use of technical and organizational measures to address compliance with the principle of data minimization.[163]

If data is processed for archiving purposes in the public interest, EU or Member State law may provide for derogations from specific provisions of the GDPR. These derogations may apply to the rights of access, right of rectification, right to restriction of processing, and right to object, to the extent that these rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of those purposes.[164]

[F] Processing for Scientific or Historical Research Purposes, or for Statistical Purposes

When data is processed for scientific or historical research purposes or for statistical purposes, appropriate safeguards must be used, consistent with the provisions of the GDPR, to ensure the protection of the rights and freedoms of the data subjects.[165] Technical and organizational measures must be used, such as pseudonymization. In addition, compliance with the data minimization principle must be ensured. If the purpose of the research can be fulfilled by using methods that do not permit or no longer permit the identification of data subjects, those purposes shall be fulfilled in that manner.

In addition, EU or Member State law may provide for derogations from the rights of access, right of rectification, right to restriction of processing, and right to object, subject to the conditions and safeguards referred above to the extent that these rights are likely to render impossible or seriously impair the achievement of the specific purposes of

163. GDPR, Art. 89(1).
164. GDPR, Art. 89(3).
165. GDPR, Art. 89(1).

the research, and such derogations are necessary for the fulfillment of those purposes.[166]

[G] Controllers or Processors Subject to an Obligation of Secrecy

Member States may adopt specific rules setting out the powers of the supervisory authority to access data, information, premises, or processing equipment, of a data controller or data processor that is subject to an obligation of professional secrecy or other equivalent obligations of secrecy.

Each Member State must notify these rules to the European Commission by May 25, 2018 and, subsequently any amendment affecting them.

[H] Rules of Churches and Religious Associations

If a church or religious association or community, at the time of entry into force of the GDPR, has comprehensive rules relating to the protection of natural persons with regard to processing of their data, these rules may continue to apply, but they must be brought in line with the GDPR. They will be subject to the supervision of an independent supervisory authority.[167]

§ 6A.15 DATA SECURITY

[A] Security of Processing

Data controllers and data processors are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of data processing.[168] The measures must take into account the nature, scope, context and purposes of the processing, the risk of varying likelihood and severity for the rights and freedoms of individuals, the state of the art, and the costs of implementation. The required measures include, as appropriate:[169]

- Pseudonymization;
- Encryption;

166. GDPR, Art. 89(2).
167. GDPR, Art. 91.
168. GDPR, Art. 32(1).
169. GDPR, Art. 32(1).

- Ensuring the ongoing confidentiality, integrity, availability, and resilience of systems and services processing personal data;
- Ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; and
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In order to maintain security and to prevent processing in breach of the GDPR, a data controller or data processor must evaluate the risks inherent in the processing and implement measures to mitigate those risks. The determination of the appropriate level of security must take into account, in particular, the risks that are presented by data processing, especially those risks that would result from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.[170]

Adherence to an approved code of conduct or an approved certification mechanism can demonstrate compliance with the above requirements.[171]

§ 6A.16 BREACH OF SECURITY

The GDPR introduces the concept of notifying individuals or the competent supervisory authority of the occurrence of a breach of security.[172] Previously, there was no blanket notification requirement applicable to all types of personal data and throughout all Member States. The GDPR brings the EU and EEA to a level comparable to numerous countries around the world.

[A] Definition of "Personal Data Breach"

The term "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration,

170. GDPR, Art. 32(2).
171. GDPR, Art. 32(3).
172. The EDPB has published guidelines on procedures surrounding the occurrence of a breach of security affecting personal data. See Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[173]

[B] Notification of the Supervisory Authority by the Data Controller

In the case of a personal data breach, the data controller must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.[174] If notification is not done within 72 hours, the data controller must provide a reasoned justification to the supervisory authority explaining the reason for the delay.

The notification to the supervisory authority must provide at least the following information:[175]

- A description of the nature of the personal data breach including where possible, the categories and approximate numbers of data subjects and data records concerned;
- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

If it is not possible to provide all of the required information at the same time, the information may be provided in phases, without undue further delay.[176]

The data controller must document any personal data breaches, including the facts surrounding the breach, its effects, and the remedial

173. GDPR, Art. 4(12). See also Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
174. GDPR, Art. 33(1). See also Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
175. GDPR, Art. 33(3).
176. GDPR, Art. 33(4).

action taken. This documentation must enable the supervisory authority to verify compliance with the controller's obligation under the applicable provisions of the GDPR.[177]

[C] Notification of a Controller by a Data Processor

A data processor that becomes aware of a personal data breach must notify the data controller without undue delay after becoming aware of a personal data breach.[178]

[D] Notification of a Data Subject by the Data Controller

The data controller is required to notify the data subjects without undue delay when the personal data breach is likely to "result in a high risk to the rights and freedoms of individuals affected." The communication to the data subject must describe in clear and plain language the nature of the personal data breach and contain at least the following information and recommendations:[179]

- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

The notification to the data subject is not required if:[180]

- The data controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the data affected by the personal data breach, in particular those that render data unintelligible to any person who is not authorized to access it, such as encryption;

177. GDPR, Art. 33(5).
178. GDPR, Art. 33(2). See also Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
179. GDPR, Art. 34(2). See also Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
180. GDPR, Art. 34(3).

- The data controller has taken subsequent measures that ensure that the high risk for the rights and freedoms of data subjects (which might have triggered the notification) is no longer likely to materialize; or
- Notification would involve disproportionate effort. In such case, the data controller must make a public communication or use a similar measure to inform the data subjects in an equally effective manner.

If the data controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the breach to result in a high risk, may require it to do so.[181]

[E] Guidelines on Personal Data Breach Notification

To assist in the interpretation and implementation of the GDPR, the EDPB has endorsed guidelines on procedures surrounding the breach of security affecting personal data. See Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01.[182]

§ 6A.17 DATA PROTECTION OFFICER

[A] Designation of a Data Protection Officer

Data controllers and data processors other than public authorities are required to designate a DPO in any case when the core processing activities of the controller or the processor consist of:[183]

- Activities that, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- Processing on a large scale of special categories of data (e.g., data pertaining to health or race) or data relating to criminal convictions and offences.[184]

---

181. GDPR, Art. 34(4).
182. The guidelines on security breach notification are available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
183. GDPR, Art. 37. See also Guidelines on Data Protection Officers (DPOs), WP243 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

The data controller or the data processor must publish the contact details of the DPO and communicate these to the supervisory authority.[185] A group of undertakings may appoint a single DPO provided the DPO is easily accessible from each establishment.[186]

[B] Required Qualifications of a Data Protection Officer

While the GDPR does not specify the qualifications required for the appointment of a DPO, it provides that the DPO should be designated based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks normally assigned a DPO.[187] The DPO may be a staff member of the data controller or data processor, or fulfill the tasks based on a service contract.[188]

[C] Position of the Data Protection Officer

The GDPR outlines the parameters for the position of a DPO in an organization and the obligations and duties that data controllers and data processors owe to the DPO.[189]

Data controllers and data processors must ensure that their respective DPO is involved, properly and in a timely manner, in all issues relating to the protection of personal data. They must support their DPO in performing the tasks assigned to them by providing the resources necessary to carry out these tasks, access to personal data and processing operations, and resources to maintain their expert knowledge.

Data protection officers are given a unique status within an organization. They directly report to the highest management level of the controller or the processor. They may not be dismissed or penalized by the data controller or the data processor for performing their tasks. The data controller or data processor must ensure that the DPO does not receive any instructions regarding the exercise of the tasks prescribed to them under the GDPR.

---

184. The terms "special categories of data" and personal data relating to criminal convictions are defined in Articles 9 and 10 of the GDPR.
185. GDPR, Art. 37(7).
186. GDPR, Art. 37(2).
187. GDPR, Art. 37(5).
188. GDPR, Art. 37(6).
189. GDPR, Art. 38. See also Guidelines on Data Protection Officers (DPOs), WP243 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

Data protection officers are bound by secrecy or confidentiality concerning the performance of their respective tasks in accordance with applicable EU or Member State law. They may fulfill other tasks and duties. However, the data controller or data processor must ensure that any such tasks and duties do not result in a conflict of interests.[190]

Article 38(4) of the GDPR grants data subjects the ability to interact with DPOs. They may contact the DPO on all issues related to the processing of their personal data and the exercise of their rights under the GDPR.

[D] Tasks of the Data Protection Officer

Data protection officers are assigned several specific tasks. These tasks include, for example:[191]

- Informing and advising the data controller or the data processor and any employees who are processing personal data of their obligations under the GDPR and other EU or Member State data protection provisions;
- Monitoring compliance with the GDPR, and other EU or Member State data protection provisions and compliance with the policies of the controller or processor regarding the protection of personal data, such as the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;
- Advising, where requested, on the conduct of a data protection impact assessment and monitoring the performance of such data protection impact assessment;
- Cooperation with the supervisory authority; and
- Acting as contact point for the supervisory authority on issues related to the processing of personal data, including prior consultation, and consulting, as appropriate, on any other matter.

[E] Guidelines on Data Protection Officers

The EDPB has endorsed Guidelines on Data Protection Officers regarding the appointment, roles, and powers of data protection

190. GDPR, Art. 38(6).
191. GDPR, Art. 39.

officers (DPOs).[192] Among other things, the DPO guidelines clarify some of the definitions that are key to determining when an organization is required, under the GDPR, to appoint a DPO. They also clarify that DPOs are not responsible for non-compliance with the GDPR. Data protection compliance is a responsibility of the data controller or data processor.

The DPO guidelines clarify the meaning of a number of key terms that are essential for determining whether, under the GDPR, a company is required to appoint a DPO. It should be reminded, however, that these definitions only apply to the requirements under the GDPR and that each Member State has the right to set additional conditions that would require companies to appoint a DPO in addition to the conditions that are set forth in the GDPR.

The DPO guidelines indicate that the term "core activities of the controller or processor" should be interpreted to relate to primary activities or key activities, and does not relate to the processing of personal data as ancillary activities. The term is not limited to companies in the data processing business. For example, the processing of data by a hospital is a "core activity" because it is essential to the operations of the hospital. On the other hand, payroll processing is not a core activity at most companies.

The guidelines clarify the meaning of "large scale." It will be determined by tangible factors such as:

- The number of data subjects concerned (specific number or percentage of the relevant population);
- The volume of data or range of different data items being processed;
- The duration, or permanence, of the data processing activity; and
- The geographical extent of the processing activity.

What constitutes "Regular and Systematic Monitoring" is also clarified by the DPO guidelines. "Regular" is defined as ongoing or occurring at particular intervals for a particular period; recurring or repeated at fixed times; or constantly or periodically taking place. "Systematic" is defined as occurring according to a system; pre-arranged, organized, or methodical; taking place as part of the general plan for data collection or carried out as part of a strategy.

192. Guidelines on Data Protection Officers (DPOs), WP243 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

The DPO guidelines also clarify the expectation regarding the requirement that the DPO should be "easily accessible from each establishment." While it is not required that the DPO work within the entity, and it is acknowledged that the DPO could be a third party, that is, someone who is not an employee of the organization. However, the DPO guidelines specify that it is essential that the data subject be able to contact the DPO. Concretely, that means the DPO must be personally available either physically being located on premises or through a hotline or other secure means of communications.

§ 6A.18 CODES OF CONDUCT AND CERTIFICATION

[A] Codes of Conduct

The GDPR encourages the drawing up of codes of conduct intended to contribute to the proper application of the GDPR.[193] These codes should take into account the specific features of the various data processing sectors and the specific needs of micro, small, and medium-sized enterprises. In particular, associations and other bodies representing categories of data controllers or data processors are invited to prepare codes of conduct, or amend or extend such codes, to specify the application of certain provisions of the GDPR, such as with regards to:

- Fair and transparent data processing;
- The legitimate interests pursued by controllers in specific contexts;
- Data collection;
- The pseudonymization of personal data;
- The information provided to the public and to data subjects;
- The exercise of the rights of data subjects;
- Information provided to, and the protection of children;
- How to collect the consent of the holder of parental responsibility for the child;
- Measures and procedures to ensure compliance with the GDPR, or compliance with the requirements for the use of data protection by design and by default, or measures to ensure security of processing;
- The notification of personal data breaches to supervisory authorities;

193. GDPR, Art. 40.

- The communication of personal data breaches to data subjects;
- The transfer of personal data to third countries outside the EU; and
- Out-of-court proceedings and other dispute resolution procedures for resolving disputes between data controllers and data subjects with respect to the processing of personal data.

These codes of conduct must contain mechanisms enabling the mandatory monitoring of compliance with its provisions by the data controllers or data processors that commit to apply it.

Entities that intend to prepare a code of conduct or to amend or extend an existing code must submit the draft code to the competent supervisory authority. The supervisory authority must then give an opinion on whether the draft code, or amended or extended code complies with the GDPR. It may approve the draft, amended or extended code if it finds that it provides sufficient appropriate safeguards.

If an approved code of conduct, or amended or extended code does not relate to processing activities in several Member States, the competent supervisory authority must register and publish the code. If the code relates to processing activities in several Member States, the competent supervisory authority must submit it to the European Data Protection Board, which must determine whether the code complies with the GDPR. The European Data Protection Board then must submit its opinion to the EU Commission.

The EU Commission may adopt implementing acts for deciding that the approved codes of conduct and amendments or extensions to existing approved codes of conduct submitted to it have general validity within the EU. These implementing acts are to be adopted in accordance with the examination procedure defined in Regulation (EU) NO. 182/2011. When the code is fully approved, the EU Commission ensures appropriate publicity for the approved codes, and the European Data Protection Board makes the code publicly available through appropriate means.

The monitoring of compliance with a code of conduct may be carried out by a body that has an appropriate level of expertise in relation to the subject matter of the code and is accredited for this purpose by the competent supervisory authority.[194]

194. GDPR, Art. 41.

[B] Certification Mechanisms

Member States, supervisory authorities, the European Data Protection Board and the EU Commission are granted the power to encourage the establishment of data protection certification mechanisms and of data protection seals and marks, for demonstrating compliance with the GDPR by processing operations carried out by data controllers and data processors.[195]

When a certification mechanism has been approved, it may issue certificates to data controllers or data processors. Certificates are valid for up to three years and may be renewed under the same conditions as long as the relevant requirements continue to be met. The European Data Protection Board is responsible for collecting all certification mechanisms and data protection seals and marks in a register and making them publicly available.

§ 6A.19 RIGHTS OF THE DATA SUBJECTS

[A] Overview of the Data Subjects' Rights

Chapter III of the GDPR is dedicated to the rights of data subjects. Data subjects are granted a wide variety of rights; including the right to:

- Obtain confirmation as to whether personal data pertaining to the data subject is being processed, and if data is processed, the purpose of the processing, categories of personal data concerned and other relevant details (right to information);[196]
- Be informed of the appropriate safeguards taken in respect of a transfer of his/her personal data to a third country (right to information);[197]
- Receive a copy of the personal data being processed by or on behalf of the data controller (right to access);[198]
- Rectification of personal data that is inaccurate (right to rectification);[199]

195. GDPR, Art. 42.
196. GDPR, Art. 15(1).
197. GDPR, Art. 15(1).
198. GDPR, Art. 15(3).
199. GDPR, Art. 16.

- Erasure of certain personal data in specified circumstances (right to erasure or right to be forgotten);[200]
- Obtain restriction of the processing of personal data in specific circumstances (right to restriction of processing);[201]
- Receive his or her personal data, which was previously provided to the data controller, in a structured and commonly used machine readable format (right to data portability);[202]
- Object to the processing of personal data concerning him or her in specified circumstances, including processing for profiling[203] and marketing purposes (right to object);[204]
- Not to be subject to a decision based solely on automated processing that produces legal effects concerning him or her, including profiling;[205]
- Obtain information regarding the details of the processing (identity and contact details of the data controller and of the data protection officer; purposes of the processing; recipients of the personal data; intention to transfer the data outside the EU/EEA territory; length of data retention);[206]
- Obtain information about his or her rights as a data subject, e.g., right of access, rectification, erasure, restriction to the processing of personal data, and portability;[207]

200. GDPR, Art. 17.
201. GDPR, Art. 18.
202. GDPR, Art. 20. See also Guidelines on the Right to "Data Portability," WP242 Rev. 01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
203. The EDPB has published Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
204. GDPR, Art. 21.
205. See also Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
206. GDPR, Art. 15(1).
207. GDPR, Art. 15(1)(e). See also Guidelines on the Right to "Data Portability" WP242 Rev. 01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

- Obtain, free of charge, information in response to the exercise of his or her rights (of information, access, erasure, etc.);[208]
- Obtain information about the right to withdraw consent;[209]
- Obtain information about the right to lodge a complaint to a supervisory authority;[210]
- Obtain information about the existence of automated decision making including profiling;[211] and
- Obtain prior notice that the controller intends to engage in further processing for a purpose other than the one for which the data was collected.[212]

[B] Data Controllers' Obligations Regarding the Exercise of the Data Subjects' Rights

Data controllers have several obligations that are linked specifically to the rights of a data subject, these include obligations for the data controllers to:

- Provide information to data subjects in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, especially when the information is addressed to a child.[213]
- Facilitate the exercise of a data subjects' rights (of information, access, erasure, etc.);[214] and
- Provide information on actions taken regarding a data subject's request regarding his or her rights (of information, access, erasure, etc.),[215] or to provide information to the data subject detailing the reasons why certain actions were not taken.[216]

208. GDPR, Art. 12(5).
209. GDPR, Art. 13(2).
210. GDPR, Art. 13(2)(d).
211. GDPR, Art. 13(2)(f); see also Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
212. GDPR, Art. 13(3).
213. GDPR, Art. 12(1).
214. GDPR, Art. 12(2).
215. GDPR, Art. 12(3).
216. GDPR, Art. 12(4).

Data controllers will have to provide means for data subjects to submit requests electronically, especially where personal data is processed by electronic means. They are also obliged to respond to a data subject's request without undue delay and not later than within one month of receiving the request, or to provide reasons for not complying with the data subject's request.[217]

Data controllers have a significant, ubiquitous obligation of providing information:[218]

- They are required to provide a data subject with information on the processing of personal data at the time of collection, or, where the data is not obtained directly from the data subject but from another source, within a reasonable period, depending on the circumstances of the case.
- If the personal data can be legitimately disclosed to another recipient, they will have to inform the data subject no later than when the data is first disclosed to the recipient.
- If the data controller intends to process the data for a purpose other than the one for which the data were collected, it must provide the data subject, before that further processing, with information on the other purpose and other necessary information as required.
- If the origin of the data cannot be provided to a data subject because various sources have been used, the data controller is required to provide the information in a general manner.

There are some exceptions.[219] The notice and information above are not required (i) if a data subject already has the information concerned; (ii) if disclosure of the data is expressly laid down by law; or (iii) where the provision of information to a data subject proves impossible or would involve disproportionate efforts, such as in the case of scientific and historical research or statistical analysis.[220]

217. GDPR, Art. 12(3).
218. GDPR, Preamble §§ 60-61.
219. GDPR, Preamble § 62.
220. Any assessment of disproportionate efforts would have to consider the number of data subjects, the age of the data, and whether adequate security and similar safeguards have been adopted.

[C] Right of Erasure or Right to Be Forgotten

Several important provisions focus on the accuracy and quality of the data. In addition to the right to have personal data concerning them rectified,[221] data subjects have the "right to be forgotten" where the retention of such data is not in compliance with the GDPR, or EU or Member State law to which the data controller is subject.

Specifically, data subjects have the right to have certain personal data erased and no longer processed in any one of the following circumstances:[222]

- The data is no longer necessary in relation to the purposes for which it was collected or processed;
- The data subject withdraws the consent on which the processing is based, or there is no other legal ground for the processing of the data;
- The data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing;
- The data has been unlawfully processed;
- The data must be erased for compliance with a legal obligation under EU or Member State law to which the data controller is subject; or
- The data pertains to a child and it has been collected in relation to the offering of information society services.

However, there are a number of exceptions to the right of erasure. These exemptions address those cases where the data is necessary (i) for exercising the right of freedom of expression and information, (ii) for compliance with a legal obligation, (iii) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, (iv) for reasons of public interest in the area of public health, (v) for archiving purposes in the public interest, (vi) for scientific and historical research purposes or statistical purposes, or (vii) for the establishment, exercise or defense of legal claims.[223]

Where a data controller has made the personal data public, it is required to inform the data controllers that are processing the data that the data subject has requested the erasure by such data controllers of any

221. GDPR, Art. 16.
222. GDPR, Art. 17.
223. GDPR, Art. 17(3).

links to, or copies or replications of that personal data. To do so, the data controller is required to take reasonable steps to communicate the data subject's request to the relevant data controllers processing the data, taking into account available technology and the means available to the controller, including technical measures.[224]

Methods to restrict processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected data unavailable to users or temporarily removing published data from a website. In automated filing systems, the restriction could be implemented though technical means, so that the data can no longer be processed, accessed, or changed. Further, the fact that the processing of personal data is restricted should be indicated in the system in such a way that it is clear that the processing of the personal data has been restricted.[225]

[D] Right to Data Portability

[1] Article 20 Right to Data Portability

Article 20 of the GDPR grants data subjects a "right to data portability."[226] Under the right to data portability, data subjects have the right to receive the personal data concerning them that they have provided to a controller, in a structured, commonly used, and machine-readable format. They also have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent or on a contract and the processing is carried out by automated means. In exercising their right to data portability, the data subjects will have the right to have their personal data transmitted directly from one controller to another, wherever technically feasible.

However, there are limits to the right to data portability. Under Art. 20(4), the right to data portability is subject to the rights and freedoms of others, and therefore, the exercise of the right to data portability may not adversely affect the rights and freedoms of others. Further, under Art. 20(3), the right cannot be exercised when the processing is necessary for the performance of a task carried out in

224. GDPR, Art. 17(2).
225. GDPR, Preamble § 67.
226. See also EDPB Guidelines on the Right to "Data Portability" WP242 Rev. 01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

the public interest or in the exercise of official authority vested in the controller.

[2] Guidelines on the Right of Portability

The EDPB Guidelines on the Right of Portability[227] confirm that the right to data portability applies only if the legal basis for the data processing is the consent of the data subject or the fact that the processing is necessary to perform a contract.

The Guidelines confirm that the exercise of the right to data portability is limited to personal data that was actively and knowingly provided by the data subject. However, the Guidelines expand the right to data portability to personal data that relates to the data subject's activity or behavior, such as personal data that are generated by, and collected from, the activities of the individual, e.g., search history, traffic data, and data location. However, according to the Guidelines, the scope of right to data portability does not include subsequent analysis of these behaviors.

The Guidelines on Data Portability clarify that the rights of the individuals include the right to receive personal data and the right to have the personal data transmitted from one data controller to another controller.

The Guidelines define the method used by data controllers to respond to a request to exercise the right of data portability. The data controller must offer, to the data subject, to directly download the data or to have the data transmitted directly to another data controller. Further, the data must be provided within one month of receipt of the data subject's request (with exceptions).

Finally, the guidelines on Data Portability specify that data controllers are not responsible for retaining personal data for longer than necessary and that the receiving controller is responsible for ensuring that the data are relevant and not excessive for the new processing.

These guidelines appear to go well beyond the wording of Article 20 of the GDPR or the intent of the drafters, as expressed in Section 68 of the Preamble to the GDPR. So far, there has not been any opportunity to evaluate this discrepancy.

227. Guidelines on the Right to "Data Portability" WP242 Rev. 01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

[E] Automated Decision Making, Including Profiling

To assist in the interpretation and implementation of the GDPR, the EDPB has endorsed Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01.[228]

§ 6A.20 REMEDIES, LIABILITIES, AND PENALTIES

[A] Right to Lodge a Complaint with a Supervisory Authority

Data subjects have the right to lodge a complaint with a supervisory authority.[229] This right is in addition to any other administrative or judicial remedy that an individual might seek.

The right to lodge a complaint may be exercised in the Member State of:

- An individual's habitual residence;
- An individual's place of work; or
- The place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the GDPR.

The supervisory authority with which the complaint has been lodged must inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.

[B] Right to an Effective Judicial Remedy Against a Supervisory Authority

Data subjects have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. This right is in addition to any other administrative or non-judicial remedy that an individual might seek.[230]

Data subjects also have the right to an effective judicial remedy where the competent supervisory authority does not handle a complaint

228. The Guidelines on Automated Individual Decision Making and Profiling for the Purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
229. GDPR, Art. 77.
230. GDPR, Art. 78(1).

or does not inform the data subject on the progress or outcome of the complaint within three months.[231]

In these cases, the proceedings against a supervisory authority are to be brought before the courts of the Member State where the supervisory authority is established.

[C] Right to an Effective Judicial Remedy Against a Controller or Processor

Data subjects have the right to an effective judicial remedy if they consider that their rights under the GDPR have been infringed because of the processing of their personal data in non-compliance with the GDPR.[232] This right is in addition to their right to exercise any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority.

The proceedings against a data controller or a data processor may be brought before the courts of the Member State where the data controller or data processor has an establishment or where the data subject has his or her habitual residence.

[D] Representation of Data Subjects

Data subjects have the right to mandate certain not-for-profit body, organizations or associations to lodge a complaint on their behalf, to exercise the rights to lodge a complaint with a supervisory authority, to have effective judicial remedy against a supervisory authority, a data controller or a data processor, and to exercise the right to receive compensation on the data subject's behalf where provided for by Member State law.[233] To quality, the not-for-profit body, organizations or associations must have statutory objectives in the public interest and be active in the protection of rights and freedoms with regard to personal data.

Further, Member States may provide that any such not-for-profit body, organization or association independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the competent supervisory authority. These entities also may exercise the rights to an effective judicial remedy against a data controller, data

231. GDPR, Art. 78(2).
232. GDPR, Art. 79.
233. GDPR, Art. 80.

processor or a supervisory authority if it considers that the rights of a data subject have been infringed as a result of the processing.[234]

[E] Suspension of Proceedings

If a competent court of a Member State has information on proceedings, concerning the same processing by the same data controller or data processor that are pending in a court in another Member State, it must contact that court to confirm the existence of such proceedings.[235]

[F] Right to Compensation and Liability

Any person who has suffered damage as a result of an infringement of the GDPR has the right to receive compensation from the data controller or data processor for the damage suffered. The basic rules of allocation of liability can be summarized as follows:

- Any data controller involved in processing is liable for the damage caused by processing that infringes the GDPR.
- A data processor is liable, as well, but only if it did not comply with its obligations under the GDPR or if it has acted outside, or contrary to, lawful instructions of the data controller.
- A data controller or data processor is not liable if it proves that it is not responsible for the event giving rise to the damage.
- If more than one data controller or data processor, or both a data controller and a data processor, are involved in the same processing and if they are responsible for any damage caused by the processing, each data controller or data processor is held liable for the entire damage in order to ensure effective compensation of the data subject.
- If a data controller or data processor has paid full compensation for the damage suffered, it is entitled to claim back from the other data controllers or data processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.

234. GDPR, Art. 80.
235. GDPR, Art. 81.

Court proceedings for exercising the right to receive compensation must be brought before the courts competent under the law of the Member State where the case is brought.

[G] Administrative Fines

[1] When Administrative Fines Are Imposed

The supervisory authority is responsible for ensuring that administrative fine assessments for infringements of the GDPR are effective, proportionate, and dissuasive.[236]

Depending on the circumstances of each individual case, administrative fines are imposed in addition to, or instead of, the measures that the supervisory authority may have taken directly, such as ordering a data controller or data processor to bring processing into compliance with the GDPR or to order a data controller to communicate a breach of security to the data subject.

When deciding whether to impose an administrative fine and the amount of the administrative fine, the supervisory authority is expected to take into account factors such as:

- The nature, gravity, and duration of the infringement, based on factors such as the nature, scope, or purpose of the processing, the number of data subjects affected, and the level of damage suffered by them;
- Whether the infringement was intentional or negligent;
- Any action taken to mitigate the damage suffered by data subjects;
- The degree of responsibility of the data controller or data processor taking into account technical and organizational measures implemented by them (e.g., data protection by design or by default, ongoing security measures);
- Any relevant previous infringements by the same entity;
- The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- The categories of personal data affected;

236. GDPR, Art. 83.

- The manner in which the infringement became known to the supervisory authority, in particular whether, and to what extent, the data controller or data processor notified the infringement;
- Adherence to approved codes of conduct or certification mechanisms; and
- Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

If an entity intentionally or negligently, for the same or linked processing operations, infringes several provisions of the GDPR, the total amount of the administrative fine may not exceed the amount specified for the gravest infringement.

[2] Amount of Administrative Fines

The GDPR defines two levels of fines. For less serious violations, the administrative fines may reach EUR 10,000,000, or in the case of an undertaking, 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. For more serious violations, the administrative fines may reach EUR 20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

[3] EUR 10 Million or 2% Annual Turn Over Fines

Infringements of the following provisions are subject to administrative fines of up to EUR 10,000,000, or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- Failure to use data processing by design and by default;
- Failure to designate a representative;
- Failure to take necessary measures to identify and oversee data processors;
- Failure to maintain records;
- Failure to use adequate security measures;
- Failure to notify of a breach of security;
- Failure to cooperate with a supervisory authority;

- Failure to perform a data protection impact assessment, if required;
- Failure to consult with a supervisory authority when required;
- Collection of personal data of children aged under 16 (or under 15,14, or 13 depending on the Member State);
- Failure to designate a data protection officer, if required;
- A certification body's failure to meet their obligations; or
- Failure to enforce commitments made under a code of conduct.

[4] EUR 20 Million or 4% Annual Turnover Fines

Infringements of other provisions are subject to administrative fines up to EUR 20 million or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. These include, for example:

- Failure to meet the basic principles for processing, including the conditions for consent;
- Infringement of data subjects' rights of information, access to their data, right of rectification, right of erasure, right to restrict the processing of their data, right to data portability, right to object to the processing of their data; right not to be subject to a decision based solely on automated processing, including profiling;[237]
- Failure to comply with the rules pertaining to the transfer of personal data to a third country;
- Failure to meet the special processing requirements regarding the processing of certain data; or
- Non-compliance with an order or a limitation on processing or the suspension of data flows by the supervisory authority.

237. The EDPB has published Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[5] EDPB Guidelines on Setting Administrative Fines

To assist in the interpretation and implementation of the GDPR, the EDPB has endorsed Guidelines on the Application and Setting of Administrative Fines for the Purpose of Regulation 2016/679, WP 253.[238]

The guidelines on administrative fines note that Recital 10 of the GDPR provides that, to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the EU, the level of protection should be equivalent in all Member States and that Recital 11 elaborates the fact that an equivalent level of protection of personal data throughout the EU requires, among others, "equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States."

The guidelines on administrative fines observe further that equivalent sanctions in all Member States, as well as effective cooperation between supervisory authorities of different Member States, is seen as a way "to prevent divergences hampering the free movement of personal data within the internal market" in line with recital 13 of the GDPR.

To ensure consistency among the supervisory authorities, the guidelines recommend that the supervisory authorities cooperate with each other and, where relevant, with the European Commission through the cooperation mechanisms as set out in the GDPR in order to support formal and informal information exchanges, such as through regular workshops. This cooperation would focus on the experience and practice of the fining powers to ultimately achieve greater consistency.

The guidelines also provide detailed guidance for the supervisory authorities on interpreting the individual facts and circumstances of the case in the light of the criteria set for in Article 83(2), i.e.:

- the nature, gravity, and duration of the infringement;
- the intentional or negligent character of the infringement;
- any action taken to mitigate the harm suffered by data subjects;

238. The guidelines are available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

- the degree of responsibility of the controller or processor, taking into account technical and organizational measures implemented by them;
- any relevant previous infringements;
- the degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- the categories of the personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor disclosed the infringement;
- where corrective measures have previously been ordered with regard to the same subject-matter and compliance with those measures;
- adherence to approved codes of conduct or approved certification mechanisms; and
- aggravating or mitigating factors, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

[6] Other Fines and Penalties

Each Member State may lay down rules on other penalties applicable to infringements of the GDPR that are not subject to the administrative fines above. Member States are required to inform the EU Commission of such additional fines by May 25, 2018.

§ 6A.21 SUPERVISORY AUTHORITY

[A] Definition

Each Member State must provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR, protecting the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the EU.[239]

239. GDPR, Art. 51.

Each supervisory authority is expected to contribute to the consistent application of the GDPR throughout the EU. For this purpose, it is expected to cooperate with each other and the EU Commission within the framework defined by the GDPR.

[B] Independence

Each supervisory authority must act with complete independence in performing the tasks and exercising the powers entrusted to it in accordance with the GDPR. The GDPR requires that the member or members of each supervisory authority remain free from external influence in the performance of their tasks and exercise of their powers.[240]

A Member State must ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the European Data Protection Board.

[C] General Conditions for the Members of the Supervisory Authority

In each Member State, the members of a supervisory authority must be appointed by means of a transparent procedure by the parliament; or by the government; or the head of State of the Member State concerned; or by an independent body entrusted by Member State law with the appointment.[241] The members of the supervisory authority must have the relevant qualifications, experience, and skills, notably in the area of protection of personal data, required to perform their duties and exercise their powers.

The duties of a member of a supervisory authority end upon the expiration of the term of office, or in case of resignation or compulsory retirement in accordance with the law of the Member State concerned. A member may only be dismissed in cases of serious misconduct or if the member no longer fulfills the conditions required for the performance of the duties.

240. GDPR, Art. 52.
241. GDPR, Art. 53.

[D] Rules on the Establishment of the Supervisory Authority

Member State are required to provide by law for the establishment of each supervisory authority; the qualifications and eligibility conditions required to be appointed as a member of the supervisory authority; and the rules and procedures for the appointment of the members of each supervisory authority.[242]

They must define the duration of the term of the member or members of each supervisory authority, whether and, if so, for how many terms the member or members of each supervisory authority shall be eligible for reappointment. Member States must define by law the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

[E] Competence

Each supervisory authority is competent to perform the tasks and exercise the powers conferred on it in accordance with the GDPR on the territory of its own Member State.[243]

[F] Tasks

Each supervisory authority is responsible for a wide range of tasks on its territory.[244] These tasks include, for example:

- Promoting public awareness of the processing of personal data and the awareness of data controllers and data processors regarding their obligations;
- Advising their national parliament, government, and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;
- Providing information, upon request, to any data subject concerning the exercise of their rights under the GDPR and, if appropriate, cooperating with the supervisory authorities in other Member States to this end;

242. GDPR, Art. 54.
243. GDPR, Art. 55.
244. GDPR, Art. 57.

- Dealing with complaints, investigating the subject matter of the complaint, and informing the complainant of the progress and the outcome of the investigation within a reasonable period;
- Cooperating with, and providing mutual assistance to other supervisory authorities to ensure the consistency of application and enforcement of the GDPR; and
- Conducting investigations on the application of the GDPR.

Additionally, a supervisory authority is responsible for the following:

- Monitoring relevant developments that impact on the protection of personal data;
- Authorizing standard contractual clauses;
- Establishing and maintaining a list of the requirement for data protection impact assessment;
- Approving binding corporate rules;
- Contributing to the activities of the European Data Protection Board; and
- Keeping internal records of breaches of the GDPR and of measures taken, in particular warnings issued and sanctions imposed.

[G] Powers

[1] Investigative Powers

Each supervisory authority has investigative powers, including, for example, the power to:[245]

- Order the data controller and the data processor, and, where applicable, their respective representative to provide any information it requires for the performance of its tasks;
- Carry out investigations in the form of data protection audits;
- Review certifications;
- Notify data controllers or data processors of alleged infringement of the GDPR;

245. GDPR, Art. 58.

- Obtain access to all personal data and to all information necessary for the performance of its tasks; and
- Obtain access to any premises, data processing equipment, and means, in conformity with Union law or Member State procedural law.

[2] Corrective Powers

The corrective powers granted to supervisory authorities include, for example, the powers to:[246] (i) issue warnings to a data controller or data processor that the intended processing operations are likely to infringe provisions of the GDPR; (ii) issue reprimands to a data controller or a data processor where processing operations have infringed provisions of the GDPR; (iii) order a data controller or data processor to comply with data subjects' requests to exercise their rights pursuant to the GDPR; (iv) order a data controller or data processor to bring processing operations into compliance with the GDPR, in a specified manner and within a specified period, or to communicate a personal data breach to the data subject; and (v) impose a limitation including a ban on processing.

Additional corrective powers include, among others, the power to (i) order the rectification, restriction or erasure of data and the notification of such actions to recipients to whom the data have been disclosed; (ii) withdraw, or order the certification body to withdraw, a certification; (iii) impose an administrative fine; and (iv) order the suspension of data transfers to a recipient in a third country or to an international organization.

[3] Authorization and Advisory Powers

Each supervisory authority is granted authorization and advisory powers, including, for example, the powers to:[247] (i) issue, on its own initiative or on request, opinions to the national parliament, the Member State government or other institutions and bodies, and to the public on any issue related to the protection of personal data; (ii) authorize processing if the law of the Member State requires such prior authorization; (iii) issue an opinion and approve draft codes of

246. GDPR, Art. 53.
247. GDPR, Art. 58.

conduct; (iv) accredit certification bodies; and (v) issue certifications and approve criteria of certification.

Each Member State also must provide by law that its supervisory authority has the power to bring infringements of the GDPR to the attention of the judicial authorities and where appropriate, to commence or engage in legal proceedings to enforce the GDPR.[248]

[H] Cooperation with Other Supervisory Authorities

[1] Mutual Assistance

The concept of "mutual assistance," provided for in Article 61 of the GDPR, includes the exchange of information among the supervisory authorities, such as responding to information requests, and the implementation of supervisory measures, such as requests to carry out prior authorizations and consultations, inspections, and investigations. Supervisory authorities are expected to provide each other with relevant information and mutual assistance in order to implement and apply the GDPR in a consistent manner.[249] They must also put in place measures to ensure effective cooperation with one another.

A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless it is not competent for the subject matter of the request or for the measures it is requested to execute. In addition, the supervisory may refuse the request if compliance with the request would be incompatible with the provisions of the GDPR or with Union or Member State law to which it is subject.

[2] Joint Operations

In some cases, the supervisory authorities may conduct joint operations such as joint investigations and joint enforcement.[250] This is the case, for example, when a data controller or data processor has establishments in several Member States or if a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations concerned.

248. GDPR, Art. 58(5).
249. GDPR, Art. 61.
250. GDPR, Art. 62.

[I] Lead Supervisory Authority

[1] Designation of a Supervisory Authority

In general, each supervisory authority is competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in the territory of its own Member State.[251] When a dispute involves an entity that operates in several Member States, in most cases, the competent "lead supervisory authority" to handle the dispute is the supervisory authority of the Member State where the controller has its main establishment.[252]

[2] Competence of the Lead Authority

If a complaint is lodged with a supervisory authority other than the lead supervisory authority, that supervisory authority is competent to deal with that complaint, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

In this case, the supervisory authority must inform the lead supervisory authority immediately on the matter concerned. Following this notification, the lead supervisory authority must decide whether it will deal with the complaint in accordance with the cooperation procedure.[253]

If the lead supervisory authority decides to deal with the complaint, the supervisory authority that originally received the complaint may submit a draft for a decision. The lead supervisory authority must take utmost account of that draft when preparing its draft decision. If the lead supervisory authority decides not to deal with the complaint, the supervisory authority that originally notified the lead supervisory authority will deal with the case in accordance with the applicable rules.

---

251. GDPR, Art. 55(1). See also Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority, WP244 rev.01; available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235.
252. GDPR, Art. 56(1).
253. The cooperation procedure is defined in GDPR, Art. 60.

[3] Cooperation Between the Lead Authority and the Other Concerned Supervisory Authorities

To avoid a scenario whereby large organizations have to deal with each of the supervisory authorities in the numerous Member States where they do business, the GDPR introduces the concept of "lead authority" and provides rules for the interaction and cooperation between the lead authority and the other concerned supervisory authorities order to reach consensus. For example:

- The lead supervisory authority and the concerned supervisory authorities must exchange all relevant information with each other.
- The lead supervisory authority may request at any time other concerned supervisory authorities to provide mutual assistance and may conduct joint operations pursuant to Article 56, in particular, for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State;
- The lead supervisory authority must communicate with the other concerned supervisory authorities, including, without delay in submitting a draft decision to the other concerned supervisory authorities for their opinion and take due account of their views.

[4] Guidelines Regarding Identification of the Lead Supervisory Authority

The EDPB has endorsed Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority, WP244 rev.01.[254] The lead authority guidelines help identify those entities that may qualify as "lead supervisory authority." Lead authorities are needed only where the data controller or processor carries out cross-border processing of personal data.

To identify the lead authority, an organization must identify the location of its main establishment or single establishment in the EU; in principle, this would be the place where the entity has its central administration. For entities with separate decision centers for different activities, there might be several lead authorities. The lead

254. Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority, WP244 rev.01; available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235.

authority guidelines provide further criteria to identifying the main establishment if the main establishment is not the place of central administration in the EU.

The guidelines also address the situation of companies that have no establishment in the EU. Data controllers that have no establishment in the EU must deal with local supervisory authority in every Member State where they have activities, through their local representative. This could make their relationship with data supervisory authorities more complex and costlier.

§ 6A.22 EUROPEAN DATA PROTECTION BOARD (EDPB)

[A] Overview

The GDPR establishes the European Data Protection Board (EDPB).[255] The EDPB is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives. It is represented by its Chair.

[B] Role of the EU Commission

The EU Commission has the right to participate in the activities and meetings of the EDPB. However, it does not have voting right. In addition, the GDPR establishes a mechanism for communications between the two organizations. It gives the Chair of the EDPB the mission to inform the EU Commission of the activities of the EDPB.

[C] Independence

The EDPB is specifically granted independence. It is expected to act independently when performing its tasks or exercising its powers.[256]

[D] Tasks Assigned to the EDPB

Article 70 provides a complete list of the tasks assigned to the EDPB. The EDPB is responsible for ensuring the consistent application of the GDPR throughout the European Union. To that end, the EDPB is empowered to take a wide range of actions on its own initiative or,

255. The European Data Protection Board is the successor of the Article 29 Working Party.
256. GDPR, Art. 69.

where relevant, at the request of the EU Commission. Their actions include, for example:

- Monitoring and ensuring the correct application of the GDPR when there is a disagreement among supervisory authorities, without prejudice to the tasks of the national supervisory authorities;
- Advising the EU Commission on any issue related to the protection of personal data in the European Union, including on any proposed amendment to the GDPR;
- Advising the EU Commission on the format and procedures for the exchange of information between data controllers, data processors, and supervisory authorities for binding corporate rules;
- Examining any question covering the application of the GDPR, and issuing guidelines, recommendations and best practices in order to encourage the consistent application of the GDPR; and
- Issuing guidelines, recommendations and best practices on procedures for erasing links, copies or replications of personal data from available communication services, under the right of erasure and right to be forgotten, or for specifying the criteria and conditions for decisions based on profiling;[257] or for establishing the criteria for evaluating data breaches or the particular circumstances in which a data controller or data processor is required to notify the occurrence of the personal data breach.[258]

[E] Annual Reports

The EDPB is tasked with the preparation of annual reports regarding the protection of individuals with respect to the processing of their personal data in the EU and, where relevant, in third countries and international organizations.[259] The report is made public and transmitted to the European Parliament, to the European Council, and to the EU Commission. Among other things, the report must include a review of the

257. The EDPB has published Guidelines on Automated Individual Decision Making and Profiling for the purpose of Regulation 2016/679, WP 251 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
258. EDPB has published guidelines on procedures surrounding the occurrence of a breach of security affecting personal data. See Guidelines on Personal Data Breach Notification under Regulation 2016/679, WP250 rev.01, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
259. GDPR, Art. 71.

practical application of the guidelines, recommendations and best practices proposed by the EDPB, and the binding decisions made by the EDPB.

§ 6A.23 CONSISTENCY

[A] Consistency Mechanism

The GDPR sets forth a "consistency mechanism" to provide a framework for the consistent application of the GDPR throughout the Member States. To this end, the GDPR requires the supervisory authorities to cooperate with each other and, where relevant, with the EU Commission, through the consistency mechanism as described below.[260]

[B] Opinion by the European Data Protection Board

There are several circumstances where the EDPB may be required to issue an opinion. In these circumstances, the EDPB must issue an opinion on the matter submitted to it unless it has already issued an opinion on the same matter. The opinion must be adopted within eight weeks by a simple majority of the EDPB members.

For example, an opinion of the EDPB may be necessary when the Chair of the European Data Protection Board or the EU Commission or a supervisory authority requests that the EDPB examine a matter of general application or a matter producing effects in more than one Member State. This could be the case, for example, if a competent supervisory authority does not comply with the obligations for mutual assistance.

An EDPB opinion may also be requested by a supervisory authority that intends to adopt certain measures, such as when it is planning to authorize new contractual clauses or binding corporate rules. In those circumstances, the supervisory authority must inform the EDPB of its proposed action, and the EDPB, in turn must issue an opinion.[261] The supervisory authority is required to "take utmost account" of the opinion of the EDPB.[262] In case of a disagreement the dispute resolution procedure described below is used.

260. GDPR, Art. 63.
261. GDPR, Art. 64.
262. GDPR, Art. 64(7).

[C] Dispute Resolution

The EDPB has the authority to adopt binding decisions in order to ensure the correct and consistent application of the GDPR in individual cases. This authority is limited to specified cases.[263] These may include, for example, if:

- A supervisory authority has expressed an objection to a draft decision of the lead supervisory authority or the lead authority has rejected an objection;
- There are conflicting views on which of the concerned supervisory authorities is competent for the main establishment; or
- A competent supervisory authority does not request the opinion of the EDPB when required, or does not follow the opinion of the EDPB. In the latter case, any supervisory authority concerned or the EU Commission may communicate the matter to the EDPB.

A decision must be adopted within one month from the referral of the subject matter by a two-third majority of the members of the EDPB. This period may be extended by a further month because of the complexity of the subject matter. If the EDPB has been unable to adopt a decision within these prescribed timeframes, it must adopt its decision within two weeks thereafter by a simple majority of the members of the EDPB, or if there is not such majority, the decision is made by the Chair.

[D] Urgency Procedure

In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, there may be derogation from the consistency mechanism or the cooperation procedure.

For example, a supervisory authority may immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity that may not exceed three months. In this case, the supervisory authority must communicate those measures and the reasons for their adoption, to the other concerned supervisory

263. GDPR, Art. 65.

authorities, the European Data Protection EDPB and to the EU Commission without delay.[264] The supervisory authority may also request that an urgent opinion or binding decision from the EDPB be made.

Any supervisory authority may also request an urgent opinion or an urgent binding decision, as the case may be, from the EDPB where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects. In making such a request, the supervisory authority must provide reasons for requesting such an opinion or decision, including the necessity for the urgent need to act.

[E] Exchange of Information

The EU Commission may adopt implementing acts of general scope for specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board.[265]

§ 6A.24 DELEGATED ACTS AND IMPLEMENTING ACTS

The EU Commission is granted the power to adopt delegated acts subject to certain conditions in Article 92. The delegated powers include: (i) the power to adopt delegated acts for determining the information to be presented by icons, and the procedures for providing standardized icons, set forth in Article 92, and (ii) the power to specify the requirements to be taken into account for the data protection certification mechanisms for demonstrating that controllers and processors processing operations comply with the GDPR.[266]

These powers are conferred on the EU Commission for an indeterminate period of time from May 24, 2016 and may be revoked at any time by the European Parliament or by the Council.

A delegated act may enter into force only if no objection has been expressed by the European Parliament or the Council within three months of notification of that act to those entities or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they have no objection.

264. GDPR, Art. 66.
265. GDPR, Art. 67.
266. GDPR, Art. 92.

§ 6A.25 ADMINISTRATIVE PROVISIONS

[A] Repeal of Directive 95/46/EC

Directive 95/46/EC is repealed, with effect from May 25, 2018.[267] The GDPR also clarifies that references to the repealed Directive 95/46/EC will be construed as references to the GDPR and that references to the Article 29 Working Party will be deemed references to the EDPB.

[B] Relationship with Directive 2002/58/EC

The relationship between the GDPR and Directive 2002/58/EC, known as the e-Privacy Directive, is clarified.[268] Specifically, the GDPR does not impose additional obligations on natural or legal persons with respect to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the European Union for matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

[C] Relationship with Previously Concluded Agreements

The GDPR briefly states that international agreements involving the transfer of personal data to third countries or international organizations that were concluded by Member States before May 24, 2016, and that comply with Union law as applicable prior to that date, shall remain in force until amended, replaced, or revoked.[269] There is no mention of the Privacy Shield or of the existing Standard Contractual Clauses.

[D] Review and Potential Amendments

The GDPR sets forth the possibility of a review and amendment of its provisions. It requires the EU Commission to submit a report by May 25, 2020 and every four years thereafter.[270] When preparing the reports, the EU Commission may request information from Member States and supervisory authorities.

---

267. GDPR, Art. 94.
268. GDPR, Art. 95.
269. GDPR, Art. 96.
270. GDPR, Art. 97.

The reports, which will be made public, are intended to provide an evaluation and review of the GDPR for the European Parliament and to the Council. They will have to examine, in particular, the application and functioning of the process and methods for the transfer of personal data to third countries or international organizations with particular regard to decisions regarding the adequacy of the protections provided by a specific country. The other items to be evaluated in the report will be the implementation of the provisions and related procedures for cooperation and consistency.

The EU Commission may also submit appropriate proposals to amend the GDPR, in particular to take into account developments in information technology and progress in the information society.

[E] Review of Other Legal Acts on Data Protection

The GDPR paves the way for amendment of other EU documents that address the protection of personal data. It requires that, when appropriate, the EU Commission submit legislative proposals to amend other European Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing.[271] This concerns, in particular, the rules relating to the protection of individuals with regard to processing of personal data by European Union institutions, bodies, offices, and agencies and the free movement of such data.

6A.26 NOTABLE ENFORCEMENT ACTIONS

[A] BunderKartellamt v. Facebook (February 2019)

In February 2019, the Bundeskartellamt - Federal Cartel Office (FCO) – Germany's competition law authority, issued an antitrust ruling against Facebook. The FCO observed that because of Facebook's dominant position on the market, users feel compelled to sign up and agree to its data handling policies regardless of the terms. It also noted that Facebook does not adequately disclose what data is collected and how it is used, making the consent, if any, provided by users not valid.

It is the first time that Facebook is being treated as a monopoly, based on the assertion that it provides a unique service for which there is no true equivalent. It is also the first case that combines privacy and

271. GDPR, Art. 98.

competition. The FCO's theory is that Facebook's dominance allows it to impose on users contractual terms that allow Facebook to track them.

The FCO examined the purpose of a small pixel, known as the Facebook Pixel, that is affixed to certain pages and transmits a wide range of user data to Facebook without the need to deploy any other Facebook service. The data collected is used to serve targeted ads to users based on their IP address. The FCO found that the disclosure lacked transparency and did not provide proper notification about the company's full scope of data collection. The FCO explained that the harm to users from the data collection is not in cost but in "loss of control".

The FCO ordered Facebook to improve the disclosures made to German users to provide more specific information and more choices on the use of their personal data in Germany. It also required Facebook to obtain consent for all of the applicable data types and uses. This obligation affects all data collected through other sites and apps such as WhatsApp and Instagram owned by Facebook. Under the GDPR, end users must explicitly consent to some uses of their personal data. The request for consent must be separate from other terms and conditions and must be clear and unambiguous. The FCO observed that Facebook users were being asked to consent to too much by simply signing up for the service

Facebook has indicated that it will appeal the decision and will argue that the FCO does not have a basis to regulate the company because its services are free to the end user and that it is not in a dominant market position because other popular social media services (such as Snapchat, Twitter and YouTube) are direct competitors of sufficient size such that no monopoly can exist in the market.

[B] CNIL v. Google (January 2019)

In January 2019, the French National Data Protection Commission (CNIL) CNIL published a "deliberation" concerning alleged violations of the GDPR by Google LLC., assessing a 50 million Euro fine to Google.[272] The investigation into Google's practices was initiated after the receipt of received complaints by two non-profit organizations regarding certain practices of Google on May 25 and May 28, 2018, shortly after the GDPR entered into force. These associations included None

272. Text of the CNIL Deliberation available at: https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1.

of Your Business ("NOYB") which is operated by Max Schrems, and La Quadrature du Net ("LQDN") a non-profit organization headquartered in France. Both complaints claimed that Google did not have a valid legal basis to process the personal data of users of its services, in particular when collecting and processing personal data to serve interest based advertising.

[1] Competence to Examine the Complaints

The GDPR establishes a "one-stop-shop mechanism," which provides that an entity established in the European Union will have as its sole interlocutor or "lead authority" the Data Protection Authority ("DPA") of the country of its main establishment.

According its published decision,[273] CNIL communicated the complaints to its European counterparts, in order to determine whether it was competent to pursue the matter in accordance with the GDPR provisions on cooperation amongst EU supervisory authorities.

In this case, after discussions with the other relevant supervisory authorities, including that of Ireland where Google's European headquarters are located, it was determined that Google did not have a main establishment in the European Union and that Google's Irish subsidiary did not have a decision-making power on the processing operations carried out in the context of the operating system Android which was the subject of the complaints. It was determined that the services were provided by Google LLC, in relation to the creation of an account during the configuration of a mobile phone, and thus, the "one-stop-shop mechanism" was not applicable. CNIL determined that it was competent to make decisions regarding processing operations carried out by Google LLC, as were the other DPA, by referring to the European Data Protection Board's (EDPB) guidelines.[274]

[2] Technical Evaluation

CNIL carried out online inspections to evaluate the processing operations identified in the Complaints. On the basis of the inspections carried out, CNIL's committee responsible for examining breaches of the Data Protection Act observed two types of breaches of the GDPR[275].

273. See Deliberation, Section I and II.
274. See Deliberation, Section II(1).
275. See Deliberation, Section II(2).

[3] Violation of the obligations of transparency and information:

CNIL determined that the information provided to Google users is not easily accessible. For example, essential information, such as the data processing purposes, the data storage periods or the categories of personal data used for the ads personalization, are disseminated across several documents, with buttons and links on which it is required to click to access complementary information. CNIL found that overall the relevant information is accessible after several steps only, for example if a user wants to have a complete information on the data collected for personalization purposes or for geo-tracking.

CNIL also found that some information is not clear or comprehensive.[276] For example, the categories of data processed, and the purposes of processing are described in a too generic and vague manner; the information is not sufficiently clear to allow the user to understand that the legal basis of processing operations for the ads personalization is the consent, and not the legitimate interest of the company. Finally, information about the retention period is not provided for some data.

[4] Violation of the obligation to have a legal basis for ads personalization processing

CNIL determined that the users are not sufficiently informed because the information on processing operations for the ads personalization is diluted in several documents and does not enable the user to be aware of their extent. For example, in the section "Ads Personalization", it is not possible to understand the plurality of services, websites and applications involved in these processing operations (Google search, You tube, Google home, Google maps, Playstore, Google pictures…) and therefore of the amount of data processed and combined.

In addition, CNIL observed that the collected consent was neither "specific" nor "unambiguous". When an account is created, while the user can modify some options. However, the choice regarding the display of ads personalization is pre-ticked.

Finally, before creating an account, the user is asked to tick the boxes « I agree to Google's Terms of Service» and « I agree to the

276. See Deliberation, Section II(2).

processing of my information as described above and further explained in the Privacy Policy» in order to create the account. Therefore, the user gives his or her consent in full, for all the processing operations purposes carried out by Google based on this consent (ads personalization, speech recognition, etc.). However, the GDPR provides that the consent is "specific" only if it is given distinctly for each purpose.

[5] The fine

CNIL imposed a financial penalty of 50 Million euros against Google indicating that the amount is justified by the severity of the infringements of the essential principles of the GDPR: transparency, information and consent, noting that the infringements observed deprive the users of essential guarantees regarding processing operations that can reveal important parts of their private life since they are based on a huge amount of data, a wide variety of services and almost unlimited possible combinations.[277] The Deliberation also observed that the violations constituted continuous breaches of the GDPR.

[6] Appeal by Google

Google has appealed the decision, arguing among other things that CNIL was not competent to evaluate the complaints.

277. See Deliberation, Section III.

NOTES

4

GDPR: One Year Later (January 21, 2019)

Ericka Watson
Danaher Corporation

DATA SUBJECT REQUESTS (GDPR ARTICLE 12-23)

The General Data Protection Regulation (GDPR) ensues that data subjects have the right to manage personal data that has been collected about them by a company (data controller). The collection use and sharing of personal data is controlled under the GDPR, and data subjects have the right to their personal data by requesting copies, making correction to ensure accuracy, limit data processing, erasure of personal data, and transport to another data controller.

Since May 25, 2018 companies have been receiving thousands of data subject requests. These requests come in various flavors, from employees requesting to exercising all rights given under the GDPR to customer's asking to be forgotten. The GDPR does not offer data subject rights as an absolute right, there are several exceptions that must be assessed to determine if fulfilling the request is appropriate. The exceptions are as follows: none of the applicable grounds on which we must delete these personal data apply per the grounds contained in Article 17(1) of the GDPR; exercising the right of freedom of expression and information; compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; for the establishment, exercise or defense of legal claims.

The GDPR states that a response must be given within 30-days of the request or an extension can be provided up to 90-days. Before responding to a request there are several two steps that must be taken. First you must verify the requestor, an ensure they are who they say they are; second work with IT and discovery tools to find the data that is maintained about the requesting data subject.

DATA TRANSFERS (GDPR ARTICLE 44-50)

The GDPR is structured to protect EU resident data no matter where it is processed. It requires that any transfer of EU personal data is done so in compliance with its requirements. Countries outside of the EU who have similarly aligned regulations and are deemed by the European Commission

to provide an adequate level of personal data protection are allowed to receive EU personal data as they are deemed adequate. However, transfers to non-adequate countries outside of the EU require an approved legal mechanism to support the transfer, such as the use of standard contractual clauses, binding corporate rules, privacy shield (US). Article 49 of the GDPR lists several derogations that permit transfers to non-adequate countries under limited circumstances.

ENFORCEMENT (GDPR ARTICLE 77-84)

GDPR enforcement has been slow and small until January 21, 2019. On this day the French Data Protection Authority issued a €50 million fine for lack of transparency. This action has started a frenzy for companies to review their privacy notices internally and externally to ensure they are clear and accurate. Please review the CNIL action below:

CNIL.

The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC

21 January 2019

On 21 January 2019, the CNIL's restricted committee imposed a financial penalty of 50 Million euros against the company GOOGLE LLC, in accordance with the General Data Protection Regulation (GDPR), for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization.

On 25 and 28 May 2018, the National Data Protection Commission (CNIL) received group complaints from the associations *None Of Your Business* ("NOYB") *and La Quadrature du Net* ("LQDN"). LQDN was mandated by 10 000 people to refer the matter to the CNIL. In the two complaints, the associations reproach GOOGLE for not having a valid legal basis to process the personal data of the users of its services, particularly for ads personalization purposes.

THE HANDLING OF THE COMPLAINTS BY THE CNIL

The CNIL immediately started investigating the complaints. On 1st June 2018, in accordance with the provisions on European cooperation as defined in the General Data Protection Regulation ("GDPR"), the CNIL sent these two complaints to its European counterparts to assess if it was competent to deal with them. Indeed, the GDPR establishes a "one-stop-shop mechanism" which provides that an organization set up in the European Union shall have only one interlocutor, which is the Data Protection Authority ("DPA") of the country where its "main establishment" is located. This authority serves as "lead authority". It must therefore coordinate the cooperation between the other Data Protection Authorities before taking any decision about a cross-border processing carried out by the company.

In this case, the discussions with the other authorities, in particular with the Irish DPA, where GOOGLE's European headquarters are situated, did not allow to consider that GOOGLE had a main establishment in the European Union. Indeed, when the CNIL initiated proceedings, the Irish establishment did not have a decision-making power on the processing operations carried out in the context of the operating system Android and

the services provided by GOOGLE LLC, in relation to the creation of an account during the configuration of a mobile phone.

As the "one-stop-shop mechanism" was not applicable, the CNIL was competent to take any decision regarding processing operations carried out by GOOGLE LLC, as were the other DPA. The CNIL implemented the new European Framework as interpreted by all European authorities in the European Data Protection Board's (EDPB) guidelines.

In order to deal with the complaints received, the CNIL carried out online inspections in September 2018. The aim was to verify the compliance of the processing operations implemented by GOOGLE with the French Data Protection Act and the GDPR by analysing the browsing pattern of a user and the documents he or she can have access, when creating a GOOGLE account during the configuration of a mobile equipment using Android.

THE VIOLATIONS OBSERVED BY THE RESTRICTED COMMITTEE

On the basis of the inspections carried out, the CNIL's restricted committee responsible for examining breaches of the Data Protection Act observed two types of breaches of the GDPR.

A violation of the obligations of transparency and information:

First, the restricted committee notices that the information provided by GOOGLE is not easily accessible for users

Indeed, the general structure of the information chosen by the company does not enable to comply with the Regulation. Essential information, such as the data processing purposes, the data storage periods or the categories of personal data used for the ads personalization, are excessively disseminated across several documents, with buttons and links on which it is required to click to access complementary information. The relevant information is accessible after several steps only, implying sometimes up to 5 or 6 actions. For instance, this is the case when a user wants to have a complete information on his or her data collected for the personalization purposes or for the geo-tracking service.

Moreover, the restricted committee observes that some information is not always clear nor comprehensive

Users are not able to fully understand the extent of the processing operations carried out by GOOGLE. But the processing operations are particularly massive and intrusive because of the number of services offered (about twenty), the amount and the nature of the data processed and combined. The restricted committee observes in particular that the purposes of processing are described in a too generic and vague manner, and so are the categories of data processed for these various purposes. Similarly, the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is the consent, and not the legitimate interest of the company. Finally, the restricted committee notices that the information about the retention period is not provided for some data.

A violation of the obligation to have a legal basis for ads personalization processing:

The company GOOGLE states that it obtains the user's consent to process data for ads personalization purposes. However, the restricted committee considers that **the consent is not validly obtained for two reasons**.

First, the restricted committee observes that the users' consent is not sufficiently informed

The information on processing operations for the ads personalization is diluted in several documents and does not enable the user to be aware of their extent. For example, in the section "Ads Personalization", it is not possible to be aware of the plurality of services, websites and applications involved in these processing operations (Google search, You tube, Google home, Google maps, Playstore, Google pictures…) and therefore of the amount of data processed and combined.

Then, the restricted committee observes that the collected consent is neither "specific" nor "unambiguous"

When an account is created, the user can admittedly modify some options associated to the account by clicking on the button

« More options », accessible above the button « Create Account ». It is notably possible to configure the display of personalized ads.

That does not mean that the GDPR is respected. Indeed, the user not only has to click on the button "More options" to access the configuration, but the display of the ads personalization is moreover pre-ticked. However, as provided by the GDPR, consent is "unambiguous" only with a clear affirmative action from the user (by ticking a non-pre-ticked box for instance). Finally, before creating an account, the user is asked to tick the boxes « *I agree to Google's Terms of Service*» and « *I agree to the processing of my information as described above and further explained in the Privacy Policy*» in order to create the account. Therefore, the user gives his or her consent in full, for all the processing operations purposes carried out by GOOGLE based on this consent (ads personalization, speech recognition, etc.). However, the GDPR provides that the consent is "specific" only if it is given distinctly for each purpose.

THE FINE IMPOSED BY THE RESTRICTED COMMITTEE AND ITS PUBLICITY

The CNIL restricted committee publicly imposes a financial penalty of 50 Million euros against GOOGLE.

This is the first time that the CNIL applies the new sanction limits provided by the GDPR. The amount decided, and the publicity of the fine, are justified by the severity of the infringements observed regarding the essential principles of the GDPR: transparency, information and consent.

Despite the measures implemented by GOOGLE (documentation and configuration tools), the infringements observed deprive the users of essential guarantees regarding processing operations that can reveal important parts of their private life since they are based on a huge amount of data, a wide variety of services and almost unlimited possible combinations. The restricted committee recalls that the extent of these processing operations in question imposes to enable the users to control their data and therefore to sufficiently inform them and allow them to validly consent.

Moreover, the violations are continuous breaches of the Regulation as they are still observed to date. It is not a one-off, time-limited, infringement.

Finally, taking into account the important place that the operating system Android has on the French market, thousands of French people create, every day, a GOOGLE account when using their smartphone. Furthermore, the restricted committee points out that the economic model of the company is partly based on the ads personalization. Therefore, it is of its utmost responsibility to comply with the obligations on the matter.

General Data Protection Regulation

GUIDE FOR PROCESSORS

SEPTEMBER 2017 EDITION

Applicable from 25 May 2018 across the whole of the European Union, the General Data Protection Regulation (GDPR) strengthens European residents' rights bearing on their data and increases accountability on the part of all stakeholders processing such data (controllers and processors), whether or not they are established in the European Union.

The Regulation lays down specific obligations that must be followed by processors, who are likely to be held liable in the event of a breach.

This guide sets out to assist processors in implementing these new obligations. All of the good practices reported by professionals may be added to it in time.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table of Contents

ARE YOU A PROCESSOR IN THE MEANING OF THE GENERAL DATA PROTECTION REGULATION? 13
ARE YOU SUBJECT TO THE GENERAL DATA PROTECTION REGULATION? 15
WHAT IS THE PRIMARY CHANGE INTRODUCED BY THE GENERAL DATA PROTECTION REGULATION FOR PROCESSORS? 16
Today 16
From 25 May 2018 16
WHAT ARE YOUR OBLIGATIONS FROM 25 MAY 2018? 17
1. A transparency and traceability obligation 17
2. Consideration of the principles of data protection by design and by default 17
3. An obligation to guarantee the security of data processed 18
4. An assistance, alert and advice obligation 19

WHERE SHOULD YOU START? 20
1. Check whether you have to designate a data protection officer 20
2. Analyse and revise your contracts 21
3. Draw up a record of processing activities 22

IF I USE ANOTHER PROCESSOR, WHAT ARE MY OBLIGATIONS? 23
DO THE CURRENT CONTRACTS WITH MY CLIENTS NEED TO BE AMENDED? 24
WHAT IS MY ROLE IN THE EVENT OF A DATA BREACH? 25
WHAT IS MY ROLE WITH REGARD TO THE IMPACT ASSESSMENT? 26
AM I ABLE TO BENEFIT FROM THE ONE-STOP-SHOP MECHANISM? 27
WHAT ARE MY OBLIGATIONS IF I AM NOT ESTABLISHED IN THE EU? 28
WHAT ARE THE RISKS IF I DO NOT COMPLY WITH MY OBLIGATIONS? 29
EXAMPLE OF SUB-CONTRACTING CONTRACTUAL CLAUSES 30

ARE YOU A PROCESSOR IN THE MEANING OF THE GENERAL DATA PROTECTION REGULATION?

You are a processor if you process personal data on behalf of, on instructions from and under the authority of a controller.

For the record, **the controller** is the person or body which "*determines the purposes and means of the processing*" (Article 4 of the GDPR – Definitions).

A **very wide variety of service providers have the capacity of processor** in the legal sense of the term. Processors' activities can concern a very specific task (sub-contracting of mail delivery) or be more general and wide-ranging (management of the whole of a service on behalf of another organisation, such as managing the pay of employees or agents for example).

The following are particularly concerned by the GDPR:

- IT service providers (hosting, maintenance, etc.), software integrators, cybersecurity companies or IT consulting companies (formerly known as IT engineering service companies/SSII in French) that have access to data,
- marketing or communication agencies which process personal data on behalf of clients, and
- more generally, any organisation providing a service which entails personal data processing on behalf of another organisation.
- A public authority or association may also be considered as such.

Insofar as they do not have access to or process personal data, software publishers and manufacturers of equipment (such as clocking terminals, biometric equipment or medical equipment) **are not concerned**.

NB:

- An organisation which is a processor is generally the controller for processing which it carries out on its own behalf, rather than for its clients (managing its own staff for example).
- When an organisation determines the purposes and means of processing, it may not be considered a processor: it shall be considered the controller of said processing (Article 28.10 of the GDPR).

Example of qualification of processor and controller

Company A provides a marketing letter delivery service using the client data files of companies B and C.

Company A is a processor for companies B and C insofar as it processes the necessary client data for sending the letters on behalf of and on instructions from companies B and C.

Companies B and C are their clients' management controllers, including as regards the delivery of marketing letters.

Company A is also the controller regarding the management of staff it employs, and the management of its clients which include companies B and C.

Tool: to determine whether you are a processor or the controller, see the Opinion 1/2010 of the Article 29 Data Protection Working Party (WP29) of 16 February 2010, which sets out the bundle of indicators to be used when **analysing on a case-by-case basis**:

- level of instructions given by the client to the service provider: what margin of manoeuvre does the service provider have in delivering its service?
- extent of monitoring over the execution of the service: to what extent does the client "supervise" the service?
- added-value provided by the service provider: does the service provider boast in-depth expertise in the field?
- degree of transparency over use of a service provider: is the service provider's identity known to the data subjects using the client's services?

Official text

Article 4 of the GDPR for the definitions of controller and processor

Article 28.10 of the GDPR on the notion of controller

ARE YOU SUBJECT TO THE GENERAL DATA PROTECTION REGULATION?

You come within the scope of the GDPR as a processor:

- **if you are established in the EU** or;
- **when you are not established in the EU**, if: your

  "*processing activities are related to*

  - *the offering of goods or services to data subjects in the EU;*
  - *or the monitoring of their behaviour as far as their behaviour takes place within the EU*"

  (Article 3 of the GDPR).

Official text

Article 3 of the GDPR on the Territorial Scope

WHAT IS THE PRIMARY CHANGE INTRODUCED BY THE GENERAL DATA PROTECTION REGULATION FOR PROCESSORS?

Today:

The obligations of the French Data Protection Act (*Loi Informatique et Libertés*) **are only enforceable as regards the controller**. Indeed, where a processor is used:

- the **contract** between said processor and the controller must indicate the **processor's obligations in terms of protecting data security and confidentiality** and stipulate that the former may only act on instructions from the latter;
- said processor must provide **sufficient guarantees** to ensure the implementation of the security and confidentiality measures set out in Article 34 of the French Data Protection Act;
- this requirement does not release the controller from its obligation to ensure compliance with such measures.

From 25 May 2018:

The GDPR establishes the **accountability principle as regards all stakeholders involved in personal data processing, from the moment such data concern European residents**, whether or not said stakeholders are established within the EU1.

It stipulates **specific obligations that must be followed by processors,** which shall particularly assist controllers in their ongoing efforts to bring their processing operations into compliance.

Official text

Articles 28, 30.2 and 37 of the GDPR on the processor's obligations

1. Recital 13 of the GDPR gives a reminder that adoption of "*a Regulation is necessary to provide legal certainty and transparency for economic operators (...), to provide natural persons in all Member States with* ***the same level of legally enforceable rights and obligations and responsibilities for controllers and processors***".

WHAT ARE YOUR OBLIGATIONS FROM 25 MAY 2018?

When you operate as a processor in the implementation of a personal data processing operation, you must provide your client with "***sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject***" (Article 28 of the GDPR).

In particular, you must assist and advise your client in its compliance with some of the obligations set forth in the GDPR (impact assessments, breach notification, security, destruction of data, contribution to audits).

In practice, this means:

1. A transparency and traceability obligation

You must:

- Draw up with your client a **contract** or other legal document specifying the obligations of each party and setting out the provisions of Article 28 of the GDPR.
- List in writing your client's instructions bearing on the processing of its data to demonstrate that you are acting "*on documented instructions from the controller*".
- Ask your client for written authorisation if, as a processor, you then engage another processor.
- Provide your client with **all necessary information for demonstrating compliance with your obligations** and for enabling the performance of audits (on the basis, for example, of the CNIL standard for the issuing of privacy seals in terms of audit procedures).
- Maintain a **record** of who your clients are and describe the processing you carry out on their behalf.

2. Consideration of the principles of data protection by design and by default

- You are obliged to provide your clients with the **necessary guarantees** that the processing you carry out on their behalf meets the requirements of the GDPR and protects the data subjects' rights. This particularly means that:

- **by design**, the tools, products, applications or services with which you provide your clients properly take on board the data protection principles, and
- **by default**, your tools, products, applications or services guarantee that only the data required for the purposes of the processing are processed, as regards the amount of data collected, the extent of their processing, the period of their storage and number of persons having access thereto.

- **To give an example**, these principles may entail:
  - allowing your client to apply default settings at the very least to data collection and not making it a technical requirement to enter data into an optional field
  - only collecting data that are strictly necessary for the purposes of the processing (data minimisation)
  - automatically and selectively clearing data from an active database at the end of a certain period, or
  - managing IT access rights and clearances on a "data-by-data" basis or at the request of the data subjects (for the social networks for example).

3. An obligation to guarantee the security of data processed

- Those of your employees who process your clients' data must be subject to a confidentiality obligation.
- You must notify your client of any breach of its data.
- You must make every effort to guarantee a level of security appropriate to the risks.
- At the end of your service and in line with your client's instructions, you must:
  - delete all data or return them to your client
  - destroy the existing copies unless there is a legal obligation to retain them.

4. An assistance, alert and advice obligation

- If you are of the opinion that an instruction from your client infringes the rules governing data protection, **you must inform the latter thereof immediately**.
- When a data subject exercises his/her rights (access, rectification, erasure, portability, to object, not to be subject to an automated individual decision, including profiling) you must, **insofar as this is possible**, **assist your client** in responding to said request.
- Given the information at your disposal, **you must assist your client** in guaranteeing compliance with the obligations bearing on the security of processing, notification of a data breach and impact assessment with regard to data protection.

WHERE SHOULD YOU START?

1. Check whether you have to designate a data protection officer

The Data Protection Officer (DPO) is tasked with overseeing compliance with the GDPR within the organisation which designated him/her.

As a processor, you will be required to designate a DPO in 2018 if:

- You are a public body or authority, or
- Your core activities involve you conducting, on your clients' behalf, regular and systematic monitoring of data subjects on a large scale, or
- Your core activities involve you processing on a large scale, on your clients' behalf, so-called "sensitive" data or data relating to criminal convictions and offences.

Over and above these compulsory cases, designation of a DPO is recommended as this way you will have an expert tasked with the practical implementation and management of compliance with the GDPR.

Examples

The guidelines on data protection officers of the WP29 adopted on 5 April 2017 provide two examples of when **it is compulsory for a processor to designate a DPO**:

Example no.1: a small family business active in the distribution of household appliances in a single town uses the services of a processor whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large scale', considering the small number of customers and the relatively limited activities. However, the activities of the processor, having many customers like this small enterprise, taken together, are carrying out large-scale processing. The processor must therefore designate a DPO under Article 37(1)(b) of the GDPR. At the same time, the family business itself is not under an obligation to designate a DPO.

Example no.2: a medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO under Article 37(1)(c), provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.

The DPO designated by a processor also oversees activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).

For more information:

See the page on this subject on the CNIL website

Official text

Article 37 of the GDPR on the obligation for a processor to designate a DPO

2. Analyse and revise your contracts

This contract must define:

- the subject-matter and duration of the service you are carrying out on your client's behalf
- the nature and purposes of the processing
- the type of personal data that you are processing on your client's behalf
- the categories of data subjects
- the obligations and rights of your client as the controller
- your obligations as the processor as set out in Article 28 of the GDPR

Clause examples

This guide gives an example of sub-contracting clauses pending the adoption of standard contractual clauses in the meaning of Article 28.8 of the GDPR. These examples of clauses can be inserted into your contracts. They must be tailored and specified according to the sub-contracting service concerned. Please note that they do not constitute a subcontract in themselves.

Official text

Recital 81 and Article 28 of the GDPR on the processor's obligations

3. Draw up a record of processing activities

As the processor, you must maintain a **record of the categories of processing activities** that you carry out on your clients' behalf.

This record must be maintained in writing and contain:

- the name and contact details of each client on behalf of which you process data
- the name and contact details of each sub-processor, where applicable
- the name and contact details of the DPO, where applicable
- the categories of processing carried out on behalf of each client
- the transfers of data outside the EU that you carry out on your clients' behalf, where applicable
- where possible, a general description of the technical and organisational security measures that you set up.

> **NB**
>
> Please also note that you are considered to be the controller for operations you carry out on your own data (for example for managing your staff or your clients) and, as such, **two records must be maintained**: one for the processing operations with regard to which you are the controller and another for the processing operations that you carry out as the processor, on your clients' behalf.

Sample record

A sample record is shown in Step 2: map your personal data processing, in the online guide General Data Protection Regulation: Getting ready in 6 steps

Official text

Article 30-2 of the GDPR on the maintenance of a record by a processor Article 30-1 of the GDPR on the maintenance of a record by a controller

IF I USE ANOTHER PROCESSOR, WHAT ARE MY OBLIGATIONS?

As a processor, you may only recruit another processor after obtaining **written authorisation from your client**. This authorisation may, at the parties' choosing, be:

- **specific**, which means granted for a specific processor, or
- **general**; you will need to inform your client of any intended change concerning the addition or replacement of processors, thereby giving your client the opportunity to object to such changes.

The processor you recruit is subject to **the same obligations as those stipulated in your contract with your controller client**. It must, in particular, provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of the GDPR.

> ***Be aware!***
>
> If the processor you recruit does not comply with its obligations, you are **fully liable** as regards the controller for this processor's compliance with its obligations.

Official text

Articles 28.2 and 28.4 of the GDPR on a processor engaging another processor

DO THE CURRENT CONTRACTS WITH MY CLIENTS NEED TO BE AMENDED?

Yes, all of the ongoing subcontracts will have to include the compulsory clauses as set out in the GDPR, on 25 May 2018.

All processors are therefore advised to:

- anticipate this change in applicable legal framework **by already incorporating, via an amendment, the clauses in ongoing contracts with their clients, whilst providing that these shall not come into force until 25 May 2018**
- conduct, from this date, **checks and/or audits** to ensure that you are complying with your obligations as a processor and to make the necessary adjustments.

Clause examples

This guide gives an example of sub-contracting clauses pending the adoption of standard contractual clauses in the meaning of Article 28.8 of the GDPR. These examples of clauses can be inserted into your contracts. They must be tailored and specified according to the sub-contracting service concerned. Please note that they do not constitute a subcontract in themselves.

WHAT IS MY ROLE IN THE EVENT OF A DATA BREACH?

A **data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

You must notify your client of any personal data breach without undue delay after having become aware of it.

On the basis of this notification, your client, as the **controller**, shall have to notify said data breach **to the competent supervisory authority** in accordance with Article 33 of the GDPR and communicate such a breach to the data subject in accordance with Article 34 of the GDPR.

Subject to your client's agreement and provided that this is clearly stipulated in the contract between you and your client, the latter may instruct you to carry out, **on its behalf**, this notification to the authority and, where applicable, to the data subjects (see clause examples at the end of this guide).

Official text:

Articles 4.12, 33 and 34 of the GDPR

WHAT IS MY ROLE WITH REGARD TO THE IMPACT ASSESSMENT?

Your client, as the **controller**, shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data in accordance with Article 35 of the GDPR. It is not, therefore, your responsibility to carry out such an assessment.

That said, you must **assist your client in carrying it out and provide any necessary information**. Said assistance must be stipulated in the contract between you and your client.

Official text:

Article 28.3 f) of the GDPR and WP29 guidelines on data protection impact assessment (p.13)

AM I ABLE TO BENEFIT FROM THE ONE-STOP-SHOP MECHANISM?

If you are established in several EU Member States, you may benefit from the one-stop-shop mechanism.

This enables bodies carrying out cross-border processing (establishments in several Member States or processing operations affecting data subjects in several Member States) to refer to a single national supervisory authority which will make decisions that are applicable to all of the Member States concerned by such processing. This authority is called the "*lead supervisory authority*".

Your lead supervisory authority will be the authority of **your main establishment**, i.e. the place of your central administration in the EU. If you do not have a central administration in the EU, this will be the establishment in the EU where the main processing activities take place.

Official text

Articles 4.16, 56 and Recital 36 of the GDPR and WP29 Guidelines for identifying a controller or processor's lead supervisory authority (p. 9)

WHAT ARE MY OBLIGATIONS IF I AM NOT ESTABLISHED IN THE EU?

If you do not have an establishment in the EU, you are subject to all of the provisions in the GDPR when:

- you process, on your client's behalf, data pertaining to data subjects within the EU
- you provide, on your client's behalf, goods or services or track the behaviour of such data subjects.

In such cases you must **designate a representative** in the EU to be the **interlocutor of the data subjects and supervisory authorities** for any question bearing on such processing.

Official text:

Articles 3 and 27 of the GDPR

WHAT ARE THE RISKS IF I DO NOT COMPLY WITH MY OBLIGATIONS?

Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive **full compensation from the controller or processor for the damage suffered**.

You may thus be held **liable for the damage suffered** and be subject to **major administrative penalties** of up to €10m or €20m depending on the category of offence or, in the event of an undertaking, up to 2% or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Said fines can apply, for example, in the following cases:

- if you act outside of your client's lawful instructions or contrary to said instructions;
- if you do not help your client to comply with its obligations (particularly notification of a data breach or performance of an impact assessment);
- if you do not provide your client with information demonstrating compliance with the obligations or enabling audits to be conducted;
- if you do not inform your client that an instruction would infringes the GDPR;
- if you engage another processor without your client's prior authorisation;
- if you engage another processor which does not provide sufficient guarantees;
- if you do not designate a DPO when this is a requirement, or
- if you do not maintain a record of the categories of processing activities you carry out on your clients' behalf.

Official text:

Articles 82 and 83 of the GDPR

EXAMPLE OF SUB-CONTRACTING CONTRACTUAL CLAUSES

The example of sub-contracting clauses below is provided pending the adoption of standard contractual clauses in the meaning of Article 28.8 of the GDPR. These examples of clauses can be inserted into your contracts. They must be tailored and specified according to the sub-contracting service concerned. Please note that they do not constitute a subcontract in themselves.

[…], located in […] and represented by […]

(hereinafter, "***the controller***")

of the one part,

AND

[…], located in […] and represented by […]

(hereinafter, "***the processor***")

of the other part,

I. **Purpose**

The purpose of these clauses is to define the conditions in which the processor undertakes to carry out, on the controller's behalf, the personal data processing operations defined below.

As part of their contractual relations, the parties shall undertake to comply with the applicable regulations on personal data processing and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which is applicable from 25 May 2018 (hereinafter "***the General Data Protection Regulation***").

II. **Description of the processing being subcontracted out**

The processor is authorised to process, on behalf of the controller, the necessary personal data for providing the following service(s) [...].

The nature of operations carried out on the data is […].

The purpose(s) of the processing is(are) [...]. The personal data processed are […].

The categories of data subjects are […].

To perform the service covered herein, the controller shall provide the processor with the following necessary information […].

III. **Duration of the contract**

This contract enters into force on […] for a duration of […] .

IV. **Processor's obligations with respect to the controller**

The processor shall undertake to:

1. process the data **solely for the purpose(s)** subject to the sub-contracting
2. process the data **in accordance with the documented instructions** from the controller appended hereto. Where the processor considers that an instruction infringes the General

   Data Protection Regulation or of any other legal provision of the Union or of Member States bearing on data protection, it shall **immediately inform** the controller thereof. Moreover, where the processor is obliged to transfer personal data to a third country or an international organisation, under Union law or Member State law to which the processor is subject, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest
3. guarantee the **confidentiality** of personal data processed hereunder
4. ensure that the **persons authorised to process the personal data** hereunder:
   - have committed themselves to **confidentiality** or are under an appropriate statutory obligation of confidentiality
   - receive the appropriate personal data protection training
5. take into consideration, in terms of its tools, products, applications or services, the principles of **data protection by design and by default**
6. Sub-contracting

   Choose one of the following two options

   ***Option A** (general authorisation)*

   The processor may engage another processor (hereinafter "***the sub-processor***") to conduct specific processing activities. In

this case, the processor shall inform the controller, in writing beforehand, of any intended changes concerning the addition or replacement of other processors. This information must clearly indicate which processing activities are being subcontracted out, the name and contact details of the sub-processor and the dates of the subcontract. The controller has a minimum timeframe of […] from the date on which it receives said information to object thereto. Such sub-contracting is only possible where the controller has not objected thereto within the agreed timeframe.

Option B *(specific authorisation)*

The processor is authorised to engage the entity […] (hereinafter the "***sub-processor***") to carry out the following processing activities: […]

Where the processor recruits other sub-processors, it must obtain the prior, specific, written authorisation of the controller.

Irrespective of the option *(general or specific authorisation)*

The sub-processor is obliged to comply with the obligations hereunder on behalf of and on instructions from the controller. It is the initial processor's responsibility to ensure that the sub-processor provides the same sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meets the requirements of the General Data Protection Regulation. Where the sub-processor fails to fulfil its data protection obligations, the initial processor remains fully liable with regard to the controller for the sub-processor's performance of its obligations.

7. **Data subjects' right to information** *Choose*

one of the following two options ***Option A***

It is the controller's responsibility to inform the data subjects concerned by the processing operations at the time data are being collected.

Option B

At the time data are being collected, the processor must provide the data subjects concerned by the processing operations with information about the data processing it carries out. The

wording and format of the information must be agreed with the controller prior to collecting the data.

8. **Exercise of data subjects' rights**

The processor shall assist the controller, insofar as this is possible, for the fulfilment of its obligation to respond to requests for exercising the data subject's rights: right of access, to rectification, erasure and to object, right to restriction of processing, right to data portability, right not to be subject to an automated individual decision (including profiling).

Choose one of the following two options

Option A

Where the data subjects submit requests to the processor to exercise their rights, the processor must forward these requests as soon as they are received by email to […] (*indicate a contact within the controller's establishment*).

Option B

The processor must respond, in the name and on behalf of the controller within the periods referred to by the General Data Protection Regulation, to data subjects' requests to exercise their rights, with regard to data covered by the sub-contracting provided for hereunder.

9. **Notification of personal data breaches**

The processor shall notify the controller of any personal data breach not later than […] hours after having become aware of it and via the following means […]. Said notification shall be sent along with any necessary documentation to enable the controller, where necessary, to notify this breach to the competent supervisory authority.

Possible option

Once the controller has agreed, the processor shall notify the competent supervisory authority (the CNIL), in the name and on behalf of the controller, of the personal data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of them, unless the breach in question is unlikely to result in a risk to the rights and freedoms of natural persons.

The notification shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Once the controller has agreed, the processor shall communicate, in the name and on behalf of the controller, the personal data breach to the data subject without undue delay where said breach is likely to result in a high risk to the rights and freedoms of natural persons.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and at least

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach,

including, where appropriate, measures to mitigate its possible adverse effects.

10. **Assistance lent by the processor to the controller regarding compliance with its obligations**

The processor assists the controller in carrying out data protection impact assessments.

The processor assists the controller with regard to prior consultation of the supervisory authority.

11. **Security measures**

The processor undertakes to implement the following security measures:

[Describe the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing]

The processor undertakes to implement the security measures set out in the [code of conduct, certification].

[Insofar as Article 32 of the GDPR provides that the controller and processor are responsible for implementing the security measures, it is recommended to precisely determine the responsibilities of each of the parties in terms of the measures to be implemented]

12. **Fate of data**

At the end of the service bearing on the processing of such data, the processor undertakes to:

At the parties' choosing:

- destroy all personal data, or

- return all personal data to the controller, or
- return the personal data to the processor designated by the controller

Together with said return, all existing copies in the processor's information systems must be destroyed. Once destroyed, the processor must demonstrate, in writing, that this destruction has taken place.

13. **The Data Protection Officer**

The processor communicates to the controller **the name and contact details of its data protection officer**, if it has designated one in accordance with Article 37 of the GDPR.

14. **Record of categories of processing activities**

The processor states that it **maintains a written record** of all categories of processing activities carried out on behalf of the controller, containing:

- the name and contact details of the controller on behalf of which the processor is acting, any other processors and, where applicable, the data protection officer;
- the categories of processing carried out on behalf of the controller;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;
- where possible, a general description of the technical and organisational security measures, including inter alia:
    - the pseudonymisation and encryption of personal data;
    - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

15. **Documentation**

The processor provides the controller with the **necessary documentation for demonstrating compliance with all of its obligations** and for allowing the controller or any other auditor it has authorised to conduct audits, including inspections, and for contributing to such audits.

V. Controller's obligations with respect to the processor

The controller undertakes to:

1. provide the processor with the data mentioned in II hereof
2. document, in writing, any instruction bearing on the processing of data by the processor
3. ensure, before and throughout the processing, compliance with the obligations set out in the General Data Protection Regulation on the processor's part
4. supervise the processing, including by conducting audits and inspections with the processor.

NOTES

5

Miriam Wugmeister, Christine E. Lyon and Cynthia Rich, Privacy Laws Around the World (May 2019)

Submitted by:
Miriam Wugmeister
Christine E. Lyon
Morrison & Foerster LLP

Miriam Wugmeister
Christine Lyon
Cynthia Rich

Morrison & Foerster LLP

May 2019

PRIVACY LAWS IN THE WESTERN HEMISPHERE (LATIN AMERICA, THE CARIBBEAN, AND CANADA)

INTRODUCTION

In Latin America, the Caribbean Canada, nineteen jurisdictions now have comprehensive privacy laws: Antigua & Barbuda, Argentina, Aruba, Bahamas, Bermuda, Brazil, Canada, Cayman Islands, Chile, Colombia, Costa Rica, Curacao, Dominican Republic, Mexico, Nicaragua, Peru, St. Maarten, Trinidad and Tobago,[1] and Uruguay. Saint Lucia adopted legislation in 2011, but the law has not yet gone into effect. Panama also reportedly enacted a new privacy law, but it is not yet published in the official gazette.

Other countries such as Bolivia, Ecuador, and Jamaica, have draft bills that have either been or are expected to be introduced to their legislatures. In addition, Argentina, Mexico and Chile have announced their intention to amend their existing laws. Argentina is proposing to amend its law to eliminate the registration requirement, make the DPA independent by separating it from any other governmental authority, and expand the legal bases for processing personal information to include the legitimate interests of the data controller. Mexico intends to introduce legislation that will regulate public and private sectors under a unified privacy law, provide for extra-territorial jurisdiction over companies that are not located in Mexico but that handle data in Mexico, strengthen existing data security requirements, require the appointment of a data privacy officer, and establish workplace monitoring rules. Chile has introduced legislation that would require registration, impose cross-border restrictions, and establish a data protection regulator.

1. On January 6, 2012, Trinidad and Tobago adopted a Data Protection Act, 2011; although, currently, the only provisions in force pertain to the establishment of the data protection authority. However, the DPA has not yet been established and there is no anticipated timeframe for its creation.

There is now a critical mass of countries in the region with privacy regimes that require, among other things, privacy notices and consents, extensive access and correction rights, database registration, and data security breach notification. While these laws impose legal obligations common to other privacy laws, particularly those found in Europe, some of the legal provisions, particularly those pertaining to cross-border transfers, are unclear and raise questions about what these requirements mean for organizations in practical terms. A careful read of the laws is imperative as they do differ from other established laws and from each other. Further, unlike the European approach, there is a heavy reliance on consent for cross-border transfers of data.

Compliance programs that comply with only EU and Asian obligations will run afoul of many of the Latin American and Caribbean country obligations.

OVERVIEW

All of the countries in the region that have enacted comprehensive data privacy laws impose a common set of data protection obligations such as notice, consent, access and correction, security, data integrity, and data retention. However, there is wider variation among the jurisdictions with respect to cross-border transfer restrictions, Data Protection Officer (DPO), data security breach notification, and registration obligations. The following summary, therefore, focuses on the major differences among these data privacy laws. Where applicable, the responsible enforcement authority and any other noteworthy characteristics specific to each jurisdiction are also highlighted.

At the end of the summary, there is a tally of the countries in the region to show at a glance the ones with mandatory cross-border, DPO, data security breach notification, and registration obligations. As the chart shows, nearly three fourths of the 19 laws in this region impose restrictions on cross-border transfers; less than half require database registration; and one half require that individuals and/or the regulator be notified in the event of a data security breach.

ANTIGUA & BARBUDA

The Data Protection Act No. 10 of 2013 ("Antigua & Barbuda Law") protects personal information of natural and legal persons and applies to processing of such data by both the public and private sectors.[2]

In Brief. *The Antigua & Barbuda Law does not require database registration, impose mandatory DPO and data security breach obligations, or restrict cross-border transfers*.

Special Characteristics

Data Protection Authority. The Information Commissioner pursuant to the Freedom of Information Act 2004 is responsible for enforcement of the Antigua and Barbuda Law. There is no website available for the Information Commissioner.

Consent. Consent is required to process personal data unless an exception applies (e.g., contractual necessity, legal obligation, or vital interests). Explicit consent is required to process sensitive personal data.

Definition of Personal Data. Personal data of natural and legal persons are defined as any information processed in the context of "commercial transactions." Such commercial transactions, whether contractual or not, include any matters relating to the supply or exchange of goods or services, investments, financing, banking, and insurance. Sensitive personal data are defined as any personal data relating to the physical or mental health or condition of a data subject, sexual orientation, political opinions, religious beliefs, or commission of criminal offenses (proven or alleged).

ARGENTINA

The Personal Data Protection Act ("Argentine Law"), enacted in 2000, protects all personal information of natural persons (living and deceased) and legal entities recorded in public or private data files, registers, and data banks, established for the purpose of providing reports.[3] Argentina was the first country, and currently only one of two countries in Latin America, to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/European Economic Area.

---

2. The Antigua & Barbuda Law is available here.
3. The Argentine Law is available in English here, and in Spanish here.

In Brief. *The Argentine Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration, and imposes detailed security requirements. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.*

Special Characteristics

Data Protection Authority. The National Directorate for Personal Data Protection ("Argentine DPA"), located within the Justice and Human Rights Ministry, is responsible for enforcement of the Argentine Law.[4]

Cross-Border Transfers. The transfer of personal information to countries outside Argentina that do not provide an adequate level of data protection is prohibited, unless the individual has provided his/her express consent to the transfer or another exception applies. In 2016, the Argentine DPA issued a list of the jurisdictions that it deemed to provide adequate protection: EEA member states, Switzerland, Guernsey, Jersey, Isle of Man, Faroe Islands, Canada (private sector only), Andorra, New Zealand, Uruguay and Israel (automatically processed data only). In addition, it issued two sets of model contractual clauses[5] for transfers to countries with inadequate data protection legislation. One set of model clauses is intended for data transfers to a data importer that is "responsible" for a data bank (i.e., a data controller). The other set of model clauses is designed to be used for data transfers to service providers. While there are many similarities between these model clauses and the EU Standard Contractual Clauses, there are also many differences, such as the inclusion of response deadlines for responding to access requests and the obligation to inform the data exporter about demands from a law enforcement authority to produce transferred data.

In December 2018, the Argentine DPA approved a set of guidelines for binding corporate rules (BCRs). Companies with BCRs that contain the information set forth in the annex to the Regulation[6] will be able to transfer personal data to inadequate countries without prior DPA approval. Companies with BCRs that differ from the conditions set forth in the Regulation will need to submit the relevant document to the Argentine DPA for approval within 30 calendar days from the date that the transfer took place.

4. The website address for the Argentine DPA is available here.
5. See Disposition 60-E/2016, available in Spanish here.
6. The Regulation is available here.

Data Security. In July 2018, Argentine DPA issued Resolution 47/2018 ("Security Guidance") which repealed the previously mandatory security requirements contained in Dispositions 11/2006 and 9/2008 related to Security Measures and updated the data security recommendations to address changes in technology and development of the Internet. The recommended security measures are contained in two Annexes to Resolution 47/2018. Annex I describes measures applicable to Computerized Data, and Annex II relates to non-Computerized Data. Annex I and Annex II each specify security measures that apply to non-sensitive personal data as well as heightened security applicable to sensitive personal data.[7]

Registration. Organizations must register their data bases with the Argentine DPA. The registration covers the processing of all personal data for all purposes.

ARUBA

The Personal Data Protection Ordinance ("Aruba Law"), enacted in 2011, establishes rules for the protection of privacy in connection with the collection and disclosure of personal information of natural persons by both the public and private sectors.[8] The Aruba Law applies to all files of data controllers established in Aruba, regardless of where such files are located (in or outside Aruba), provided that the files contain personal information of individuals settled in Aruba.

In Brief. *The Aruba Law imposes restrictions on cross-border transfers but does not require database registration, the appointment of a DPO, and data security breach notification*.

Special Characteristics

Data Protection Authority. The Minister of Justice is responsible for enforcement of the law.[9]

Cross-Border Transfers. The Aruba Law prohibits transfers of personal information into the files to which the law is not applicable, to the extent that the Minister has declared that such transfers would result in a serious disadvantage for individuals' privacy. The Minister can issue a waiver for files located outside Aruba if the law of the

7. Resolution 47/2018 is available here.
8. The Aruba Law is available here.
9. The website address for the Aruba Ministry of Justice is here.

country in which the file is located provides an equivalent level of privacy and data protection.

BAHAMAS

The Data Protection (Privacy of Personal Information) Act 2003 ("Bahamas Law") protects personal information of natural persons and applies to processing of such data by both the public and private sectors.[10]

In Brief. *The Bahamas Law does not require database registration, impose mandatory DPO and data security breach obligations, or restrict cross-border transfers. However, with respect to the latter three areas, the DPA has issued non-binding guidance. In addition, the Bahamas Law is unusual because there are no explicit notice and consent requirements*.

Special Characteristics

Data Protection Authority. The Office of the Data Protection Commissioner ("Bahamas DPA") is responsible for investigating any contraventions of the Bahamas Law, either of his own volition or as a result of a complaint by an individual concerned.[11]

Notice and Consent. While there are no explicit notice and consent requirements set forth in the Bahamas Law, the Bahamas DPA interprets the obligation to collect and process personal information fairly to mean that individuals must be made aware of certain information regarding the processing of their personal information, and must consent to that processing, or one of the other conditions specified in the Bahamas Law must apply.

Cross-Border Transfers. The Bahamas DPA has the authority to prohibit the transfer of information outside the Bahamas where there is a failure to provide protection either by contract or otherwise equivalent to that provided under the Bahamas Law. The Bahamas DPA has issued nonbinding guidance listing the conditions, similar to those found in EU laws, which need to be met to transfer personal information cross-border.

Data Protection Officer. There is no obligation under the Bahamas Law to appoint a DPO; however, the Bahamas DPA recommends it.

---

10. The Bahamas Law is available by navigating the Government website portal at here.
11. The website of the Bahamas DPA can be found by navigating the website portal of the Bahamas Government. The portal address is here.

Data Security Breach Notification. There is no obligation on organizations to give notice in the event of a data security breach; however, there is voluntary DPA Guidance on Managing a Data Security Breach. The Guidance states that organizations may choose to provide notice in the event of a breach of security resulting in unauthorized access to, or alteration, disclosure or destruction, or accidental loss or destruction of personal information.

BERMUDA

The Personal Information Protection Act, 2016 ("Bermuda Law"), enacted in August 2016, applies to public and private sector organizations that use personal information in Bermuda.[12] The government announced at the time that there would be a period of approximately two years before the Bermuda Law entered into force; however, as of February 2019, the Bermuda is still not yet in force.

In Brief. *The Bermuda Law restricts cross-border transfers and requires data security breach notification and the appointment of a DPO. However, there are no database registration requirements*.

Special Characteristics

Data Protection Authority. The Office of Privacy Commissioner ("Bermuda DPA") will be responsible for enforcement of the Bermuda Law.

Cross-Border Transfers. An organization may transfer personal information to a jurisdiction that has been recognized by the government as providing a comparable level of protection or to an overseas third party where the organization reasonably believes it provides comparable protection (e.g., the overseas third party has adopted a DPA-recognized certification mechanism). Otherwise, the organization must use contractual mechanisms, corporate codes of conduct including binding corporate rules, or other means to ensure a comparable level of protection.

Data Protection Officer. An organization must designate a representative ("data protection officer") for purposes of compliance with the Bermuda Law. The DPO will have primary responsibility for communicating with the Bermuda DPA.

12. The Bermuda Law is available here.

Data Security Breach Notification. Where there is a breach of security that leads to the loss or unlawful destruction or unauthorized disclosure of, or access to, personal information which is likely to adversely affect an individual, the organization responsible for that personal information must, without undue delay, notify the Bermuda DPA of the breach and then any individual affected by the breach.

BRAZIL

Law No 13,709 of August 14, 2018 ("Brazilian Law") regulates the processing of personal data, including via digital means, by individuals or legal entities (public and private).[13] The Brazilian Law is expected to enter into force in August 2020.

In Brief. *The scope and the requirements of the Brazilian Law are very similar to the scope and requirements of the GDPR. For example, the legal bases required for processing and the cross-border rules are largely consistent with the GDPR. However, with respect to Individual Rights, DPO, and breach notification requirements, the Brazilian Law exceeds GDPR requirements*.

Special Characteristics

Data Protection Authority. In December 2018, the outgoing administration of the President issued an Executive Order 869/2018 creating the Brazilian Data Protection Authority ("Brazilian DPA").

Scope. The Brazilian Law applies to processing that takes place within Brazil as well as extraterritorially where the processing has the goal of offering or providing goods or services or processing the data of individuals located in Brazil.

Cross-Border Transfers. To transfer to a third country, the country must be recognized as providing adequate protection or there must be in place standard contractual clauses or binding corporate rules (BCRs), unless another legal basis applies.

Individual Rights. Like the GDPR, the Brazilian law provides similar access, correction, deletion, and data portability rights. However, the obligations with respective to response times, frequency of requests, and the ability to charge fees are more onerous. For example, there is

13. The Brazilian Law is available here (in Portuguese).

no limit on the frequency of requests and requests for access must be responded to within 15 days.

Data Protection Officer. A DPO must be appointed and the identity and contact information must be made publicly available.

Data Security Breach Notification. The **data** controller must inform the Brazilian DPA and individuals of the occurrence of security incidents that could entail relevant risk or damage to individuals. Notice must be made within a reasonable period, as defined by the Brazilian DPA, and must include certain information specified under the Brazilian Law.

CANADA

The Personal Information Protection and Electronic Documents Act ("Canadian Law") regulates the collection, use, and disclosure of personal information of natural persons by private sector organizations for commercial purposes, with limited exceptions (e.g., where the organization is handling personal information in a province with substantially similar provincial legislation and the organization is provincially regulated).[14]

In the context of an employment relationship, the collection, use, and disclosure of employees' personal information by an employer is covered only where the employer is a private-sector Federal Work, Business or Undertaking, meaning a federally regulated entity (e.g., organizations in the transportation, communications, broadcasting and banking sectors). Canada is regarded as providing an adequate level of protection for personal data transferred from the EU/EEA.

In Brief. *The Canadian Law requires the appointment of a DPO and breach notification. However, there are no cross border restrictions or special security or registration requirements*.

Special Characteristics

Data Protection Authority. The Privacy Commissioner of Canada ("Canadian DPA") is responsible for investigating complaints, conducting audits, and pursuing court action under two federal laws. It also publicly reports on the personal information-handling practices of public and private sector organizations and promotes public awareness

14. The Canadian Law is available here.

and understanding of privacy issues. The Canadian DPA does not have the authority to order compliance, award damages, or levy penalties.[15]

Cross-Border Transfers. There are no express limitations in the Canada Law on cross-border transfers. In fact, the Canadian Law does not distinguish between domestic and international transfers of data. However, any organization that has transferred personal information to a third party (including an affiliate) for processing generally remains responsible for that personal information. The organization that transfers personal information to any foreign service provider must use contractual or other means to provide comparable level of protection while personal information is in possession of foreign entity.

Data Breach Notification. In June 2015, Parliament passed amendments to the Canadian Law requiring mandatory breach notification, which became effective November 1, 2018. Organizations are required to report to the Canadian DPA and notify affected individuals of a breach where the breach poses a "real risk of significant harm" to affected individuals. Organizations must also notify government institutions and other organizations in prescribed circumstances, including where the organization believes that the government institution or other organization may be able to reduce or mitigate the risk of harm to affected individuals.

Data Protection Officer. Organizations must appoint an individual or individuals who are accountable for the organization's compliance with the Canadian Law. Although other individuals within the organization may be responsible for the day-to-day processing of personal information, accountability rests with the designated individual.

CAYMAN ISLANDS

Data Protection Law, 2017 ("Cayman Islands Law") will come into force in September 2019.[16] The Cayman Islands Law applies to private sector controllers established or not established in the Cayman Islands that process personal data in the Cayman Islands. The data controller not established in the Cayman Islands must nominate a local representative established in the Islands

In Brief. *The Cayman Islands Law does not require registration or the appointment of a DPO. However, the Cayman Islands Law restricts cross-*

15. The website address for the Canadian DPA is here.
16. The Cayman Islands Law is available here.

border transfers and requires notification in the event of a data security breach.

Special Characteristics

Data Protection Authority. The Office of the Ombudsman ("Cayman Islands DPA") will be responsible for enforcement of the law when it takes effect on September 30, 2019.[17]

Cross-Border Transfers. Personal data must not be transferred to a country or territory unless that country or territory ensures an adequate level of protection or an exception applies. Authorization from the Cayman Islands DPA is not required for cross border transfers. However, under the Law, the Cabinet may, after consultation with the Cayman Islands DPA and others, make regulations prescribing the types of processing that require prior DPA approval (e.g., processing that is considered particularly likely to cause substantial damage or substantial distress to individuals).

Data Security Breach Notification. Controllers must notify affected individuals and the Cayman Islands DPA without undue delay where there is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or, access to, personal data transmitted, stored, or otherwise processed.

CHILE

Law No. 19.628 of Protection of Personal Data ("Chilean Law"), the first privacy law enacted in Latin America in 1999, regulates the processing of personal information of natural persons by both the public and private sectors.[18]

In Brief. The Chilean Law does not restrict cross-border transfers or impose data security breach notification, DPO or registration requirements. Unlike most privacy laws, the Chilean Law does not establish a DPA to oversee enforcement; civil courts are responsible for enforcing the law.

17. The website address for the Cayman Islands DPA is here.
18. The Chilean Law is available here.

COLOMBIA

Enacted in October 2012, Law No. 1581 "Introducing General Provisions for Personal Data Protection" ("Colombian Law") sets forth general rules for the protection of personal information of natural persons by both the public and private sectors, including special protections for children.[19] The Colombian Law is intended to compliment a law enacted in 2008 that applies to personal credit information only.

In Brief. *The Colombian Law imposes DPO, data security breach notification, and registration requirements and restricts cross-border transfers to countries that do not provide adequate protection*. *In addition, some additional data security measures are required*.

Special Characteristics

Data Protection Authority. The Personal Data Protection Division ("Colombian DPA"), the organization within the Superintendence of Industry and Commerce responsible for performing the functions of the DPA, is authorized to carry out investigations on the basis of complaints or on its own initiative.[20]

Cross-Border Transfers. The transfer of personal information to countries outside Colombia that do not provide an adequate level of data protection is prohibited, unless the individual has provided his/her express to the transfer, the transfer is necessary to execute a contract between the individual and the organization or another exception applies. The DPA may approve transfers to non-adequate countries that do not fall under one of the above-listed exceptions by issuing a conformity declaration ("declaración de conformidad"). The additional requirements and obligations that must be satisfied before the Colombian DPA may issue such declarations are expected to be addressed in the forthcoming implementing regulations. In August 2017, the Colombian DPA issued a list of countries that, in its view, provide adequate data protection.[21]

Data Protection Officer. Every organization and service provider must appoint a person or department responsible for protecting personal information and processing requests from individuals who seek to exercise their rights under the law.

---

19. The Colombian Law is available in Spanish here.
20. The website address for the Colombian DPA is here.
21. The DPA's External Circular No. 5 is available here.

Data Security. In May 2015, the Colombian DPA issued voluntary accountability guidelines which set out high level procedures for developing a data management program. Apart from these guidelines, the Colombian DPA has indicated that it does not intend to issue regulations that prescribe detailed security measures. Instead, it expects organizations to demonstrate accountability by implementing measures that are relevant and appropriate for their respective businesses.

Data Security Breach Notification. Both the organization and the service provider must inform the Colombian DPA about any violations of security codes and any risks in the administration of information of individuals. There is no obligation to give notice of such breaches directly to individuals.

Registration. In November 2015, the Colombian DPA launched its online database registration process. The registration process proceeded in stages, based on the last digits of the Colombian company's tax identification number ("NIT"). Organizations and service providers that carry out processing of personal information in Colombia must register. It is quite unusual to require service providers to file registrations with the DPA.

COSTA RICA

Law No. 8968 on the Protection of the Person Concerning the Treatment of Personal Data ("Costa Rican Law") came into force on September 5, 2011.[22] It applies to automatic and manual processing of personal information of natural persons by both public and private entities. In December 2016, the law was amended[23] to eliminate the controversial concept of a "Super User" which gave the data protection authority (Prodhab) the right to gain unrestricted access to registered databases. In addition, the amendments introduced new definitions that clarify, among other things, that databases used for internal purposes (e.g., human resources databases), including those shared with affiliated entities do not need to be registered with the regulator, and that sharing of personal information with affiliated entities and agents do not constitute a transfer which would trigger the need for consent.

In Brief. *The Costa Rican Law requires data security breach notification and registration. It also imposes special data security but does*

22. The Costa Rican Law is available in Spanish here.
23. See Executive Decree No. 40008-JP in Spanish here, starting on page 9.

not require the appointment of a DPO or restrict cross-border transfers. However, there are general rules that apply to all data transfers.

Special Characteristics

Data Protection Authority. Prodhab ("Costa Rican DPA"), established in March 2012, is responsible for creating a database registry, ensuring compliance with the Costa Rican Law, and issuing implementing regulations.[24]

Cross-Border Transfers. There are no limitations on cross-border transfers; however, the general rules for any transfer of databases and/or personal information apply. In particular, express written consent (or a contract) is required to share or transfer personal information. The Costa Rican Law does not include any other legal bases for transferring data and this rule applies broadly to all transfers without explicit indication of whether the transfer occurs within or outside Costa Rica.

Data Security. In addition to the basic security obligations, the Costa Rican Law requires organizations to issue a "Performance Protocol" that will regulate all the measures and rules to be followed in the collection, management and handling of the personal information. In order to be considered valid, the Performance Protocol (and any subsequent amendments) must be registered with the Costa Rican DPA.

Data Security Breach Notification. Organizations must inform individuals about any irregularities in the processing or storage of their personal information, or when the organization becomes aware of such irregularities. Irregularities include but are not limited to loss, destruction, and/or misuse that result from a security vulnerability or breach. They must inform individuals within five working days from the time the vulnerability occurs, so the individuals may take appropriate action.

Registration. Every database that is established for distribution, promotion or commercialization purposes must be registered with the Costa Rican DPA. Databases used for internal purposes (e.g., human resources databases), including those shared with affiliated entities do not need to be registered.

24. The website address for the Costa Rican DPA is here.

CURACAO

The Personal Data Protection Act ("Curacao Law"), which took effect October 1, 2013, regulates the processing of personal information of natural persons by both the public and private sectors.[25] The Curacao Law is modeled on the Dutch Data Protection Law.

In Brief. *The Curacao Law restricts the cross-border transfer of personal information to countries that do not provide adequate protection. However, there are no DPO, data security breach notification, and registration requirements. There is also no required time frame specified for responding to access or correction requests.*

Special Characteristics

Data Protection Authority. The College Bescherming Persoonsgegevens ("Curacao DPA") supervises compliance with the Act.[26]

Cross-Border Transfers. Personal information may only be transferred to a country outside the Kingdom if that country ensures an adequate level of protection. Where there is no adequate level of protection the data transfer may take place provided that:

- the individual has provided his/her explicit consent;
- the transfer is necessary for the performance of a contract between the individual and the data controller or for actions to be carried out at the request of the individuals and which are necessary for the conclusion of a contract;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the data controllers and third parties in the interests of the individuals;
- the transfer is necessary on account of an important public interest, or for the establishment, exercise or defense in law of any right;
- the transfer is necessary to protect the vital interests of individuals;
- the transfer is carried out from a public register set up by law or from a register which can be consulted by anyone or by any persons who can invoke a legitimate interest, provided that in the case concerned the legal requirements for consultation are met.
- the transfer has been approved by the Curacao DPA.

25. The Curacao Law is available in Dutch here.
26. The website address for the Curacao DPA is not available.

DOMINICAN REPUBLIC

The Organic Law 172-13 on the Protection of Personal Data ("Dominican Law") took effect on December 13, 2013.[27] The Dominican Law protects personal information filed in public or private archives, public records, and data banks intended to provide reports. The Dominican Law also regulates Credit Information Companies and the provision of credit reference services and the supply of information on the market to ensure respect for privacy and the rights of the information owners.

In Brief. *In contrast to the cross-border rules found in other countries in the region, the Dominican Law imposes a common set of legal bases for all international transfers, regardless of their destination. Registration/ supervision requirements apply only to public or private databanks that are intended to provide credit reports. Such databanks are subject to the inspection and supervision of the Superintendence of Banks. There is also no obligation to appoint a DPO or to notify individuals or the regulator in the event of a data security breach. The Dominican Law does not establish a DPA to oversee compliance; however, the Superintendence of Banks is the entity authorized to regulate Credit Information Companies.*

Special Characteristics

Cross-Border Transfers. Personal information may only be transferred internationally in certain circumstances such as:

- The individual consents to authorize the transfer of information or when the laws so allow;
- The transfer is necessary for the execution of a contract between the individual and the organization, or for the execution of pre-contractual measures;
- The transfer concerns bank or security transfers, with regard to the respective transactions and in accordance with the applicable legislation;
- The transfer has been agreed or considered in the framework of international treaties or conventions, or in free-trade treaties of which the Dominican Republic is a part;

27. The Dominican Law is available in Spanish here.

- The transfer of legally required information is to safeguard public interest or for the acknowledgement, exercise or defense of a right in a judicial process, or is required by a tax or customs administration to fulfill its duties.

MEXICO

The Federal Law on Protection of Personal Data Held by Private Parties ("Mexican Law"), enacted in 2010, regulates the process of personal information of natural persons by private sector organizations but does not apply to duly licensed credit reporting companies.[28]

In Brief. *The data protection rules in the Mexican Law have a number of important differences from those found elsewhere in the region. For example, the notice and data security obligations are subject to detailed rules. Unlike many laws in the region, the Mexican Law does not require registration but it does require the appointment of a DPO and data security breach notification. In addition, domestic and international transfers are largely subject to the same requirements.*

Special Characteristics

Data Protection Authority. The Federal Institute for Access to Information and Data Protection ("Mexican DPA") is responsible for disseminating information on data protection and compliance with the Mexican Law.[29]

Notice. In 2013, the DPA issued Guidelines that provide for three different types of Privacy Notices: comprehensive, simplified and short. A comprehensive Privacy Notice must always be made available; however, depending on the circumstances of the data collection, a simplified or short Privacy Notice may be provided first. The Guidelines state expressly that provision of a simplified or short Privacy Notice does not relieve the organization of its obligation to make available a comprehensive Privacy Notice.

Simplified or Short Privacy Notice. Where personal information is obtained directly from the individual by any electronic, optical, audio or visual means, or through any other technology, the organization must immediately provide the individual with at least the information

28. The Mexican Law is available in English here.
29. The website address of the Mexican DPA is here.

regarding the identity and domicile of the organization and the purposes of the data processing, as well as provide the mechanisms for the individual to obtain the full text of the Privacy Notice. Where cookies, web beacons or similar technologies are used, a communication or warning must be placed in a conspicuous place to inform the individual about the use of these technologies and how the technology can be disabled by the individual.

Data Protection Officer or Office. The Mexican Law requires any entity that collects personal information to appoint a DPO or office to promote the protection of personal information within its organization and process requests (such as access and correction requests) received from individuals who wish to exercise their rights under the Mexican Law.

Data Security. The Regulations, issued in 2011, define what constitutes physical, technical and administrative measures and, in particular, require the establishment of an internal supervision and monitoring system, implementation of a training program for personnel to educate and generate awareness about their obligations to protect personal information, and external inspections or audits to check compliance with privacy policies. The list of security measures must be updated when security improvements or changes are made or there are breaches of the systems. In addition, the organization is encouraged to consider undertaking a risk analysis of personal information to identify dangers and estimate the risks for the personal information, conduct a gap analysis and prepare a work plan to implement the missing security measures arising from the gap analysis.

Whenever there is a security violation involving personal information, the Mexican may take into account the organization's compliance with DPA recommendations to determine the attenuation of the corresponding sanction.

Data Security Breach Notification. Security breaches that occur "at any stage of processing that materially affect the property or moral rights" of the individual must be reported to the individual by the organization so, the individual can take appropriate action to protect his or her rights. The Mexican Law does not require notice to any public authority or regulator.

NICARAGUA

Nicaragua enacted the Law on Personal Data Protection on March 21, 2012 (Act No. 787) and the Regulation of the Law on Personal Data Protection (Decree No. 36-2012) ("Nicaraguan Law") on October 17, 2012.[30] The Nicaraguan Law protects personal information of natural and legal persons in private and public databases.

In Brief. *The Nicaraguan Law restricts cross-border transfers and requires registration; however, the registration procedure is not yet established. Data security breach notification and the appointment of a DPO are not required. Unlike other laws in the region, the Nicaraguan Law has a provision of the right to "digital oblivion."*

Special Characteristics

Data Protection Authority. The Nicaraguan Law calls for the creation of a Directorate for Personal Data Protection within the Ministry of Finance that will be responsible for the regulation, supervision, and protection of processing of personal information; however, as of March 2017, the Directorate has not yet been established. The Directorate will be responsible for a wide range of data protection related activities, including issuing regulations, monitoring compliance, and imposing administration sanctions in the event of violations.

Cross-Border Transfers. The assignment and transfer of personal information to countries or international organizations that do not provide adequate security and protection for personal information are prohibited except in very limited circumstances, such as where:

1) the transfer is for the purposes of international judicial cooperation;
2) the exchange of personal information is for health matters;
3) the transfer is necessary to carry out epidemiological investigations, wire transfers or exchanges;
4) the transfer is required by law;

30. The Nicaraguan Law is available in Spanish here; the Regulation is available in Spanish here.

5) the transfer is agreed upon under any international treaties ratified by Nicaragua; or

6) the transfer pertains to international cooperation with intelligence agencies or to criminal matters covered by specified laws.

Such transfers must be carried at the request of a legally authorized person, the request must state the object and purpose of the intended processing, the organization must comply with the data security and confidentiality measures and verify that the receiving organization complies equally with these measures, the individual is informed about and consents to the transfer by the organization, and the intended purposes of the processing.

Right to Digital Oblivion. The Nicaraguan Law is one of the first laws to include the right to be forgotten, which has been so controversial in the EU. In particular, the individual has the right to request that social networks, browsers, and servers suppress or cancel his or her personal information contained in their databases. In the case of databases of public and private institutions that offer goods and services and collect personal information for contractual reasons, individuals may request that their personal information be cancelled once the contractual relationship ends. This provision is not particularly detailed and it is not clear how organizations will implement these obligations.

PERU

The Law for Personal Data Protection ("Peruvian Law"), which protects personal information of natural persons processed by public and private sector organizations, entered into force July 4, 2011; however, many of the provisions and its Regulations did not become effective until May 2013.[31] Organizations had until March 2015 to conform their existing Personal Data Banks to the Peruvian Law.

In Brief. *The Peruvian Law requires registration and restricts cross-border transfers*. *The Peruvian DPA has also established data security breach notification requirements*. *There is no obligation to appoint a DPO*.

Special Characteristics

Data Protection Authority. The Peruvian Law established the National Authority for Protection of Personal Data ("Peruvian DPA")

31. The Peruvian Law is available in Spanish here.

to oversee compliance and, in particular, administer and keep up-to-date the National Register of Personal Data Protection, hear and investigate complaints lodged by individuals, issue provisional and/or corrective measures, and impose administrative sanctions in cases of violations.[32]

Cross-Border Transfers. Cross-border transfers of personal information are allowed if the recipient has adequate data protection as may be determined by the Peruvian DPA. Thus far, the Peruvian DPA has not issued a list of adequate recipients. The Peruvian Law provides certain exceptions to this provision, including where the transfer of personal information is necessary to complete a contract to which the individual whose information is being transferred is a party; where the individual has given consent; or where otherwise established by regulation issued under the Peruvian Law.

The Regulations additionally provide that cross-border transfers are permitted when the importer assumes the same obligations as the exporting organization. The exporter may transfer personal information on the basis of contractual clauses or other legal instruments that prescribe at least the same obligations to which the exporter is subject as well as the conditions under which the individual consented to the processing of his or her personal information. Therefore, if a contract is in place, consent or one of the other legal bases listed above would not be required.

Authorization for cross-border transfers is not required; however, the organization and the service provider may request the opinion of the Peruvian DPA as to whether the proposed transfer of personal information cross-border meets the provisions of the Peruvian Law.

Data Security Breach Notification. The Peruvian Law itself does not impose data security breach notification requirements; however, it authorizes the Peruvian DPA to establish the security requirements and conditions to be met by data controllers. In October 2013, the Peruvian DPA issued an Information Security Directive that instructs data controllers to notify individuals of "any incidents that significantly affect their proprietary or moral rights."

Registration. All organizations must register with the Peruvian DPA. In addition, organizations that voluntarily adopt codes of conduct to govern their transfers to affiliated entities must register them with the Peruvian DPA.

---

32. The website address of the Peruvian DPA is here.

ST. MAARTEN

The Personal Data Protection National Ordinance (St. Maarten Law), enacted in 2010, regulates the processing of personal information of natural persons by both the public and private sectors.[33]

In Brief. *The St. Maarten Law restricts cross-border transfers but does not impose registration, data security breach notification or DPO requirements*.

Special Characteristics

Data Protection Authority. The Personal Data Protection Supervisory Committee ("St. Maarten DPA") is responsible for supervising compliance with the Ordinance.[34]

Cross-Border Transfers. Personal data may be sent to another country only if that country guarantees an appropriate level of protection; otherwise, transfers to a country without an appropriate level of protection may take place only if there is a legal basis for the transfer such consent or contractual necessity or the St. Maarten DPA issues a permit for the transfer.

URUGUAY

Law No. 18.331 on the Protection of Personal Data and Habeas Data Action ("Uruguayan Law"), enacted in 2008 and amended in 2010, regulates the processing of personal information of natural and legal persons by both the public and private sectors.[35] Uruguay was the second country in South America to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/EEA.

In Brief. *The Uruguayan Law requires data security breach notification and registration and restricts cross-border transfers to countries that do not provide adequate protection. There is no requirement to appoint a DPO; however, the person responsible for the database is liable for violations of the provisions of the law and his or her name will be identified in the registration*.

33. St. Maarten Law is available here.
34. The website address for the St. Maarten DPA is not available.
35. The Uruguayan Law is available in Spanish here.

Special Characteristics

Data Protection Authority. The Regulatory and Control Unit for the Protection of Personal Data ("Uruguayan DPA") was created as an entity decentralized from the Agency for the Development of Government of Electronic Management and Information Society and Knowledge ("AGESIC").[36]

Cross-Border Transfers. The transfer of personal information of any kind to countries or international organizations that fail to provide adequate levels of protection according to the standards of Regional or International law in this area is prohibited except where the following cases apply:

- international judicial cooperation, according to the relevant international instrument, whether Treaty or Convention, subject to the circumstances of each case;
- exchange of medical data, when necessary for the treatment of the sick person and due to reasons of public health or hygiene;
- bank or stock exchange transfers, as regards to the corresponding transactions and pursuant to the applicable legislation;
- agreements within the framework of international treaties to which the Republic of Uruguay is a party; and
- international cooperation between intelligence agencies fighting against organized crime, terrorism and drug trafficking.

It also is possible to make international transfers of data in the following cases:

- the interested party has given his consent to the proposed transfer;
- the transfer is necessary for the execution of a contract between the interested party and the person responsible for the processing or to implement pre-contractual measures taken at the interested party's request;
- the transfer is necessary to execute an agreement entered into now or hereafter on behalf of the interested party, between the person responsible for the processing and a Third Party;

36. The website address of the Uruguayan DPA is here.

- the transfer is necessary or legally required to safeguard an important public interest, or for the recognition, exercise or defense of a right in a legal procedure;
- the transfer is necessary for safeguarding the vital interests of the interested party; or
- the transfer is effected from a record which, by virtue of legal or regulatory provisions, is designed to provide information to the public and is open to consultation by the general public or any person who can prove a legitimate interest, provided that the conditions established by law for consultation are met in each particular case.

Regardless of the cases listed above, the Uruguayan DPA may authorize a transfer or a series of transfers of personal information to a third country that does not guarantee an adequate level of protection, when the person responsible for the processing offers sufficient guarantees regarding the protection of privacy, fundamental rights and freedoms of individuals, as well as to the exercise of the corresponding rights.

Such guarantees may arise from appropriate contractual clauses.

Data Security Breach Notification. When the data controller or the data processor realizes that there has been a data security breach which could affect the individual's rights in a significant way, the data controller or the data processor must inform the individual.

Registration. All organizations that create, modify, or eliminate databases of personal information must register their Databases.

AMERICAS MANDATORY REQUIREMENTS				
COUNTRIES WITH PRIVACY LAWS	**REGISTRATION**	**DPO[37]**	**CROSS-BORDER LIMITATIONS**	**DATA SECURITY BREACH NOTIFICATION[38]**
19	**6**	**5**	**13**	**9**
Antigua & Barbuda	No	No	No	No
Argentina	**Yes**	No	**Yes**	No
Aruba	No	No	**Yes**	No
Bahamas	No	No	No	No
Bermuda	No	**Yes**	**Yes**	**Yes**
Brazil	No	**Yes**	**Yes**	**Yes**
Canada (Federal)	No	**Yes**	**No**	**Yes**
Cayman Islands	No	No	**Yes**	**Yes**
Chile	No	No	No	No
Colombia	**Yes**	**Yes**	**Yes**	**Yes**
Costa Rica	**Yes**	No	No	**Yes**
Curacao	No	No	**Yes**	No
Dominican Republic	No	No	**Yes**	No
Mexico	No	**Yes**	No	**Yes**
Nicaragua	**Yes**	No	**Yes**	No
Peru	**Yes**	No	**Yes**	**Yes**
St. Maarten	No	No	**Yes**	No
Trinidad & Tobago (law not yet fully in force)	No	No	**Yes**	No
Uruguay	**Yes**	No	**Yes**	**Yes**

37. In some jurisdictions, the appointment of a Data Privacy Officer (DPO) may exempt the organization from its registration obligations.
38. This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

Miriam Wugmeister
Christine Lyon
Cynthia Rich

Morrison & Foerster LLP

May 2019

PRIVACY LAWS IN ASIA (EAST, CENTRAL, AND SOUTH) AND THE PACIFIC

INTRODUCTION

Fourteen jurisdictions in this region now have comprehensive privacy laws: Australia, Hong Kong, India, Japan, Kazakhstan, Kyrgyzstan, Korea, Macao, Malaysia, New Zealand, the Philippines, Singapore, Taiwan, and Turkmenistan. While all of these laws are based on the core data protection principles, the specific rules are quite different from each other and from laws found in other parts of the world. For example, unlike their European, Latin, and African counterparts, countries in Asia have largely eschewed registration requirements. However, like their European, Latin, and African counterparts, many are increasingly embracing cross-border restrictions and breach notification obligations.

Notably absent from this list are countries such as China, Indonesia, Thailand, and Vietnam. China has not yet enacted a comprehensive privacy law but the country does have sector-specific regulations, as well as the Cyber Security Law, which became effective June 1, 2017. In addition to regulating network security, the CSL includes broad provisions governing the protection of network data, including personal information and a data localization requirement that requires that operators of "key information infrastructure" (KII) to store in China both personal data and "significant data" collected and produced in the course of business operations in China.

Similarly, Indonesia does not have a comprehensive data privacy law but the country enacted regulations in December 2016 in connection with its Electronic Information and Transaction Law that established protections for personal data transmitted through electronic media. The government of Thailand has drafted legislation but it has not been approved yet by the legislature. Vietnam also appears to be moving slowly toward the development of privacy legislation.

Given the variances among these new privacy laws, businesses with operations in the region will want to re-examine their privacy policies and

practices to ensure they will comply with these new regimes. Compliance programs that comply only with the more established Asian or European regimes will run afoul of many of these new country obligations.

OVERVIEW

All of the jurisdictions in the region that have enacted comprehensive data privacy laws impose a common set of data protection obligations such as notice, consent, access and correction, security, data integrity, and data retention. However, there is wider variation among the jurisdictions with respect to cross-border transfer restrictions, Data Protection Officer (DPO), data security breach notification, and registration obligations. The following summary, therefore, focuses on the major differences among these data privacy laws. Where applicable, the responsible enforcement authority and any other noteworthy characteristics specific to each jurisdiction are also highlighted.

In addition, given the wide scope of application of China's Cybersecurity Law, a brief summary of some of the law's key privacy provisions is also provided.

At the end of the summary, there is a tally of the countries in the region to show at a glance the ones with mandatory cross-border, DPO, data security breach notification, and registration obligations. As the chart shows, three fourths of the fourteen laws in this region impose restrictions on cross-border transfers; one third require the appointment of a DPO and data security breach notification.

AUSTRALIA

Australia's Privacy Act 1988 (Cth) ("Australian Law") has been amended three times since it was enacted, first in 2000, then again in 2012 and most recently in 2017. In February 2017, the Privacy Amendment (Notifiable Data Breaches) Bill 2016[39] was enacted. The legislation, which became effective on February 22, 2018, requires organizations to give notice to the regulator and affected individuals when a data breach has occurred.

In Brief. *The Australian Law imposes restrictions on cross-border transfers and requires notification in the event of a data security breach. Registration and the appointment of a DPO are not required; however, the Privacy Commissioner recommends that organizations appoint a DPO.*

39. The Privacy Amendment (Notifiable Data Breaches) Bill 2016 is available here.

Special Characteristics

Data Protection Authority. The Australian Law is administered by the Privacy Commissioner in the Office of the Australian Information Commissioner ("Australian DPA").[40] The Australian DPA has the power to conduct privacy compliance assessments of Australian Government agencies and some private sector organizations, accept enforceable undertakings, and seek civil penalties in the case of serious or repeated breaches of privacy.

Application of the Act. One of the significant changes to the Australian Law is the extension of the APPs to cover overseas handling of personal information by an organization if it has an "Australian link." An organization has an Australian link if the organization is:

- an Australian citizen; or
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law; or
- a partnership formed in Australia or an external Territory; or
- a body corporate incorporated in Australia or an external Territory; or
- an unincorporated association that has its central management and control in Australia or an external Territory.

An organization that falls within one of the above categories will also have an Australian link where:

- the organization carries on business in Australia or an external Territory;
- the personal information was collected or held by the organization in Australia or an external Territory, either before or at the time of the act or practice.

According to the DPA's guidelines, activities that may indicate that an entity with no physical presence in Australia carries on business in Australia include:

40. The website address for the Australian DPA is here.

- the entity collects personal information from individuals who are physically in Australia;
- the entity has a website which offers goods or services to countries including Australia;
- Australia is one of the countries on the drop down menu appearing on the entity's website; or
- the entity is the registered proprietor of trademarks in Australia.

Where an entity merely has a website that can be accessed from Australia is generally not sufficient to establish that the website operator is "carrying on a business" in Australia.

Employee Records. The existing exemption for employee records covering "acts or practices in relation to employee records of an individual if the act or practice directly relates to a current or former employment relationship between the employer and the individual," remains intact; the intention is to revisit this issue in subsequent rounds.

Cross-Border Transfers. Before disclosing personal information to a recipient overseas, organizations must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information received, except where one of the following situations applies:

- The recipient is subject to a law or binding scheme that protects the information in a substantially similar manner, and there are mechanisms available to the individual to enforce that protection; or
- The individual is expressly informed that, if he or she consents to the disclosure of the information, the organization is relieved of its obligation to take the required reasonable steps above to ensure that the overseas recipient does not breach the APPs, and, after being so informed, the individual consents to the disclosure; or
- The disclosure of the information is required or authorized by or under an Australian law or a court/tribunal order; or
- There is an exception under the law that covers the disclosure of the information by the organization.

The cross-border rules apply to transfers by the organization to its overseas affiliates but not an overseas office.

Data Protection Officer. There is no obligation to appoint a Data Protection Officer; however, there is a general obligation to implement appropriate practices, procedures, and systems to comply with

the APPs. The APP guidelines cite the example of designated privacy officers as a possible governance mechanism to ensure compliance with the APPs.

Data Security Breach Notification. The Australian Law requires that the Australian DPA and affected individuals be notified of data breaches. An eligible data breach is defined as "unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity" where "the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates". In February 2018, the Australian issued Data Breach Guidance, which outlines key requirements relating to data breaches, including personal information security requirements and the obligations of the mandatory requirements, as well as addresses other key considerations in developing a robust data breach response strategy.[41]

CHINA

China's Cyber Security Law ("CSL"), which became effective June 1, 2017, applies to the construction, operation, maintenance and use of Networks, as well as supervision and administration of Network Security in China. The CSL's privacy and data security provisions are likely to apply to a wide range of organizations that either own or use a computer information network (effectively to all personal information in electronic form).[42]

In addition, the Information Security Techniques – Personal Information Security Specification ("Privacy Standard") was issued on December 29, 2017, and took effect on May 1, 2018.[43] The Privacy Standard is a non-binding, recommended national standard that expands on the CSL's data privacy and security requirements. The Privacy Standard will likely be influential in regulatory authorities' interpretation of the CSL, but it is unclear how or if the Privacy Standard will be enforced.

In Brief. *The CSL applies only to Network Operators and operators of Critical Information Infrastructure. Consent is the only legal basis on which to collect, use or disclose personal information. Individual rights are limited to correction and deletion; no access requirements are specified. In addition, the CSL imposes special rules with respect to security, DPO, data localization, and breach notification.*

41. Australia's Data Breach Guidance is available here.
42. China's CSL is available here.
43. The Privacy Standard is available here.

Special Characteristics

Data Protection Authority. The Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology of PRC (MIIT), and the Ministry of Public Security of the PRC (MPS) are responsible for enforcement of the CSL.[44]

Scope. The CSL applies to Network Operators and operators of critical information infrastructure ("CII"). A "Network Operator" is defined as "the owner and administrator of a network and network service provider." A "network" broadly defined as "a system of computers or information terminals that collect, store, transmit, exchange and process information." Interpreted broadly, Network Operator could apply to any company in China that operates a computer network in the course of its business. "CII Operator" is not defined. Rather, "CII" is defined as networks and systems that: (i) are used for important industries, such as public communications and information services, energy, transportation, water resources, finance, public utilities, and e-government affairs; and (ii) if suffering damage, loss of function or data breach, "might seriously endanger national security, national welfare and people's livelihood, or the public interest." Examples of CII operators include banks (e.g., ICBC), telecom carriers (e.g., China Telecom), utility companies (e.g., State Grid) and insurance companies (e.g., China Life).

Data Protection Officer. Network Operators must designate a responsible person in charge of Network Security and implement the responsibility for Network Security. CII Operators must set up a dedicated security management body and designate a responsible person in charge of security management.

Legal Basis for Processing. Consent is required to collect, use or disclose a user's personal information.

Data Security Breach Notification. The CSL requires that remedial measures be taken immediately, users be promptly informed, and relevant reports be submitted to the competent departments by the impacted entity as set forth under the CSL. In addition, Network Operators must develop an emergency response plan to Network Security incidents so as to promptly deal with security risks, such as system vulnerabilities, computer viruses, Network attacks and Network intrusions.

---

44. The website address for the CAC is here; the website address for the MIIT is here; and the website address for the MPS is here.

Data Localization. CII Operators must store in China both personal information and "important data" collected and produced in the course of business operations in China. It is not yet clear if the data localization provisions would also apply to Network Operators, defined as parties who own or administer a computer network in China and network services providers (companies providing licensed telecommunications services over the network).

HONG KONG

Hong Kong was the second jurisdiction in Asia to enact a comprehensive data protection law in 1995. The Personal Data (Privacy) Ordinance ("Hong Kong Law") protects all personal information of natural persons and applies to both the private and public sectors.[45] The Hong Kong Law was amended in 2012, and one of the most significant changes was to more closely regulate the use and provision of personal information in direct marketing activities. In addition, certain changes to the data protection principles were made, new offenses and penalties were introduced, the authority of the Privacy Commissioner for Personal Data was enhanced, and a new scheme whereby it may provide legal assistance to individuals was introduced. The majority of the changes went into effect on October 1, 2012; the new direct marketing and the legal assistance provisions took effect on April 1, 2013.

In Brief. *The Hong Kong Law does not require the appointment of a DPO, data security breach notification, or registration; however, the Privacy Commissioner does recommend that organizations appoint a DPO and provide notice in the event of a data security breach. The Hong Kong Law contains a provision that restricts cross-border transfers to countries that do not provide adequate protection; however, the provision is not in force*.

Special Characteristics

Data Protection Authority. The Office of Privacy Commissioner for Personal Data ("Hong Kong DPA") is responsible for enforcement.[46]

Cross-Border Transfers. While the Hong Kong Law contains a provision (Section 33) that limits the transfer of personal information to a place outside Hong Kong that does not provide data protection

45. The Hong Kong Law is available here. The 2012 Amendment is available here.
46. The website of the Hong Kong DPA is here.

similar to that under Hong Kong Law, it is not yet in force, and there is no schedule as to when it will come into force. Consequently, transfers both within and outside Hong Kong are governed by general legal restrictions on data collection and data use.

In December 2014, the Hong Kong DPA issued voluntary guidance to help organizations understand their compliance obligations under Section 33. The guidance contains a set of recommended model data transfer clauses for such transfers. The Hong Kong DPA has called upon the government to implement Section 33 and has also developed and submitted to the Administration a white list of 50 jurisdictions that, in his view, provide similar protection. If and when Section 33 is implemented, the transfers to jurisdictions on the white list would be exempted from the requirements under Section 33.

Data Protection Officer. There is no statutory requirement to appoint a DPO. However, the Hong Kong DPA recommends it. Appointment of a DPO is a common business practice in Hong Kong.

Data Security Breach Notification. There is no legal obligation on any entities to give notice in the event of a data security breach under the Hong Kong Law; however, the Hong Kong DPA issued voluntary guidance which recommends that organizations "seriously consider" notifying individuals affected by a breach where there is a real risk of harm. Organizations may also choose to notify the Hong Kong DPA.

Marketing. One of the most significant changes was to more closely regulate the use and provision of personal information in direct marketing activities. Under the new direct marketing rules, an organization can only use or transfer personal information for direct marketing purposes if that organization has provided the required information (notice) and consent mechanism to the individual concerned and obtained his or her consent. "Consent" in the direct marketing context includes an indication of no objection to the use (or provision); however, written consent is required prior to providing personal information to others for their direct marketing purposes. Failure to comply with these requirements is a criminal offense, punishable by fines of HK$500,000 and three years' imprisonment. In cases involving transfer of personal data for gain, a fine of HK$1,000,000 and five years' imprisonment are possible.

INDIA

In 2011, India issued final regulations implementing parts of the Information Technology (Amendment) Act, 2008 dealing with protection of personal information. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Indian Privacy Rules") prescribe how personal information may be collected and used by virtually all organizations in India, including personal information collected from individuals located outside of India.[47]

Efforts are underway to develop new and more comprehensive privacy rules. A data protection bill was proposed in the government and reviewed by India's Ministry of Electronics and Information Technology in 2017. A public consultation was held on the draft bill in August 2018.

In Brief. *The Indian Privacy Rules do not require the appointment of a DPO, data security breach notification*[48]*, or registration. There are restrictions on cross-border transfers, but they apply only to sensitive personal information. Furthermore, as explained below, outsourcing providers are subject to a narrower set of obligations, the consent obligations only apply to sensitive information, and sensitive information is very broadly defined.*

Special Characteristics

Data Protection Authority. The Ministry of Electronics & Information Technology (previously known as the Ministry of Communications and Information Technology) is responsible for enforcement of the Indian Privacy Rules.[49]

Application of the Rules. The Indian Privacy Rules raised significant issues and caused concern among organizations that outsource

47. The Indian Privacy Rules are available here.
48. There are breach notification requirements, however, set forth in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("Rules"). Under these Rules, notice must be provided to the Indian Computer Emergency Response Team ("CERT-in") in the event of certain Cyber Security Incidents specified under the Rules. The Rules apply to all electronic Information (data, text, images, sound, voice, codes, computer programs, software and databases or microfilm or computer generates micro fiche) and all individuals, organizations or corporate entities affected by Cyber Security Incidents involving a computer, computer system, computer network, data, computer data base or software located in India.
49. The website address of the Indian Ministry is here.

business functions to Indian service providers. As drafted, the Indian Privacy Rules apply to all organizations that collect and use personal information of natural persons in India regardless of where the individuals reside or what role the company that is collecting the information plays in the process of handling the information. In particular, the provisions apply to a "body corporate," which is defined as "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities," as well as, in many instances, "any person on its behalf." As a result, industry both within and outside India expressed concern that the Indian Privacy Rules would decimate the outsourcing industry.

In response to these concerns, on August 24, 2011, the Indian Ministry of Communication & Technology issued a clarification of the Indian Privacy Rules ("Clarification"), stating that the Indian Privacy Rules apply only to organizations in India.[50] Therefore, if an organization in India receives information as a result of a direct contractual relationship with an individual, all of the obligations under the Indian Privacy Rules continue to apply. However, if an organization in India receives information as a result of a contractual obligation with a legal entity (either inside or outside India), e.g., is acting as a service provider, the substantive obligations of notice, choice, data retention, purpose limitation, access, and correction do not apply, but the security obligations and the obligations relating to the transfer of information do apply.

Consent. The consent rules apply only to sensitive information.

Sensitive Information. Sensitive information is very broadly defined and includes information that is not generally regarded as sensitive in other jurisdictions. In particular, it is defined as "information relating to: (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise; provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law

50. The Clarification is available here.

for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."

Cross-Border Transfers. An organization may transfer sensitive personal information to any organization or person in India or to another country that ensures the same level of data protection. The transfer may only be allowed if it is necessary for the performance of the contract between the organization (or its agent) and the individual or where the individual has consented to the transfer.

JAPAN

In September 2015, Japan enacted legislation to amend the country's 2005 Personal Information Protection Act ("Japanese Law"),[51] which regulates the handling of personal information of natural persons by private sector organizations. The amendments, which went into effect on May 30, 2017, made significant changes to the ways in which companies handle personal information, particularly with respect to disclosures to third parties, international transfers, anonymously processed information, and the collection and use of sensitive personal information. The amendments also provided for the creation of the Personal Information Protection Commission, an independent authority charged with overseeing data protection compliance.

Effective January 2019, the Japanese Law is now recognized by the European Commission as providing adequate protection for personal information.

In Brief. *The Japanese Law imposes restrictions on cross-border transfers and sets forth special rules for sharing personal information with third parties and using anonymized information. The appointment of a DPO and data breach notification are required in the financial services sector and recommended in all other sectors. There are no registration requirements, however.*

Special Characteristics

Data Protection Authority. The Personal Information Protection Commission ("Japanese DPA"), an independent government authority, is responsible for overseeing data protection compliance. Previously

51. The Japanese Law is available here.

the national administrative agencies and local governments were responsible for enforcement.[52]

Anonymized Information. The recent amendments and the rules issued by the Japanese DPA create new requirements for the creation and use of anonymized processed information. If a company deletes certain information that may identify individuals from personal information and creates anonymized processed information in accordance with the amended law, the company may use anonymized processed information for any purposes and transfer such anonymized processed information to any third parties. There are also specific rules for companies that anonymize data, including when transferring anonymized information to a third party, publicly announcing the items of information included in the anonymized information to be provided and the method of the provision, and notifying the third party that the transferred information is or contains anonymized information.

Cross-Border Transfers. Prior to the 2015 amendments, the Japan Law did not impose limitations on cross-border transfers; however, the rules for disclosures to third parties did apply. Now, under the amendments, express consent or a data transfer agreement, or intercompany rules in the case of affiliated entities, are required to transfer personal information to foreign third parties (including affiliated entities) except where the transfer is to a third party in a country that provides equivalent protection or where the foreign third party has an internal personal information protection system equivalent to that which is required for domestic organizations under the amended law.

As of January 23, 2019, the Japanese Law was recognized by the European Commission as providing adequate protection for personal information. To obtain the EU Commission's adequacy decision, Japan enacted additional safeguards ("Supplemental Rules") around the processing of personal information received from the EU. The Supplemental Rules are binding on organizations that receive personal information transferred from the EU based on an adequacy decision and are thus required to comply with them.

Data Protection Officer. Although the Japanese Law does not require the appointment of a DPO, a DPO is required in the financial and credit sectors and, in all other sectors, the Japanese DPA recommends that organizations appoint a person in charge of handling personal data as part of their security measures.

---

52. The website address of the Japanese DPA is here.

Data Security. Organizations must adopt measures necessary and appropriate for preventing the divulgence, loss, or damage of personal information and otherwise control the security of that information. In addition, some of the guidelines impose more extensive security requirements, including encryption and service provider supervision.

Data Security Breach Notification. Data breach notification is not explicitly addressed in the recent amendments but is addressed in guidelines for the financial sector. These guidelines which remain in force require organizations in this sector to report to the regulators information regarding data breaches and remedial measures taken in the event of a leakage of personal information. In addition, the Japanese DPA has issued guidance applicable to all sectors that recommends that organizations report relevant facts and remedial measures to the Japanese DPA (or competent minister if so specified by the Japanese DPA) in the event of a leakage, loss, or damage of personal information, except for some minor incidents (e.g., if there was no substantial harm because the leaked information was retrieved before it could be reviewed by third parties). Data breach reporting forms are available on the Japanese DPA website.

Joint Use Notice. If an organization intends to jointly use personal information with third parties (including corporate affiliates), it must provide information on the scope of joint users, items of personal information to be jointly used, purpose of joint use, and the name of the individual or entity primarily responsible for the management of the data. The information must be provided through a notice to the individual or by placing the individual in circumstances whereby he or she can easily find out. Any change in purposes of joint use and/or the name of the individual or entity primarily responsible for the management of the data must also be reported to the individuals or publicly announced.

Opt-Out Notification. Organizations may disclose non-sensitive personal information to third parties without obtaining opt-in consent if the organizations provide the requisite prior notice to individuals and notify the Japanese DPA. The requirement to notify the Japanese DPA is one of the changes under the amendments. In addition, the use of this opt-out notification procedure for disclosures involving any sensitive personal information is now prohibited.

Sensitive Information. Under the amended Japanese Law, sensitive personal information is now defined and subject to different collection, use, and disclosure rules. In particular, organizations must

obtain individuals' express consent at the time sensitive personal information is collected unless one of the limited exceptions applies.

KAZAKHSTAN

The Law on Personal Data and Protection ("Kazak Law"),[53] which went into effect in November 2013, protects all personal information of natural persons and applies to both the private and public sectors. The law was amended in November 2015 to impose new data localization requirements, effective January 2016.

In Brief .*The Kazak Law restricts cross-border transfers to countries that do not protect personal information. It also imposes data localization requirements and exceedingly short timeframes for responding to access and correction requests*. *However, there are no data breach notification, special security, DPO, or registration requirements*.

Special Characteristics

Data Protection Authority. There is no independent data protection authority responsible for enforcement of the Kazak Law. In practice, the General Prosecutor's Office and its territorial bodies are authorized to investigate and initiate administrative cases involving data protection law violations; the Ministry of Internal Affairs and the Ministry of Finance are responsible for investigating and initiating criminal cases involving data protection law violations.

Access and Correction Access requests must be acted upon within three working days; correction requests must be acted upon within one day.

Cross-Border Transfers Personal information may be transferred without restriction to a country that protects personal information. However, to transfer personal information to a country that does not provide such protection, consent or another one of the very limited exceptions must apply.

Data Localization Effective January 1, 2016, companies established in Kazakhstan as well as representative offices and branches of foreign companies that own or operate databases containing personal information must store personal information in Kazakhstan. It is unclear,

53. The Kazak Law is available here.

however, if this storage requirement applies to foreign companies without any legal presence in Kazakhstan whose operations are aimed at Kazakhstan and whose websites are accessible in the territory of Kazakhstan (e.g., Internet companies).

KYRGYZSTAN

The Law on Personal Data ("Kyrgyz Law"),[54] which went into effect in April 2008, protects all personal information of natural persons and applies to both the private and public sectors.

In Brief. *The Kyrgyz Law restricts cross-border transfers, requires database registration (not yet in force), and imposes exceedingly short timeframes for responding to access and correction requests. In addition, similar to laws in the EU, the Kyrgyz Law requires organizations to have a legal basis for processing personal information such as consent, legitimate interests, vital interests, or legal requirements. However, the Kyrgyz Law does not impose data breach notification, special security, or DPO requirements.*

Special Characteristics

Data Protection Authority The Kyrgyz Law requires the government to designate a specific state body to regulate the collection and use of personal information, handle registrations, maintain records of personal data files and holders of such files, and make international agreements on the crossborder transfer of personal information. The State Registration Service, the public authority responsible for, among other things, implementing the country's informatization policy and supervising business activities and programs in this sector, has some but not all of the DPA functions set forth in the law. In particular, the State Registration Service has not been given authority over the registration process for personal data holders.

Access and Correction Requests Access and correction requests must be fulfilled within seven days. Cross-Border Transfers Personal information may not be transferred to countries that do not provide an adequate level of protection unless one of the limited exceptions applies such as consent or vital interests. Legal Basis for Collection and Use Similar to EU law, the Kyrgyz Law requires organizations to have a

54. The Kyrgyz Law is available here.

legal basis for processing personal information such as: the individual has consented to the processing (consent); the processing is necessary to pursue a legitimate interest of the organization (legitimate interests), the processing is necessary to protect the vital interests of the individual (vital interests), or the processing is necessary to comply with a legal requirement (legal requirement). Registration Companies must register with their personal data files with the DPA; however, as of May 2017, the government has yet to designate a state authority responsible for registration.

MACAO

The Personal Data Protection Act ("Macao Law"), which took effect in 2006, was the first jurisdiction in Asia to adopt an EU-style data protection law.[55] Virtually all of the provisions (notice, consent, collection and use, data security, data integrity, data retention, access and correction, cross-border limitations, and registration) closely follow the requirements found in EU laws. The Macao Law applies to both public and private sector processing of personal information of natural persons. Macao was the first jurisdiction in the region to require registration and impose EU-style cross-border restrictions.

In Brief. *The Macao Law imposes restrictions on cross-border transfers that mirror EU cross-border restrictions and requires registration of databases*. *It does not require the appointment of a DPO or data security breach notification*.

Special Characteristics

Data Protection Authority. The Office for Personal Data Protection ("Macao DPA") is responsible for enforcement.[56]

Registration. Registration is required unless an exemption applies.

MALAYSIA

The Personal Data Protection Act ("Malaysian Law") was enacted in 2010 but did not come into effect until November 2013; organizations were given three months (until February 15, 2014) to comply.[57] The Malaysian Law

55. The Macao Law is available in Chinese and Portuguese here.
56. The website address of the Macao DPA is here.
57. The Malaysian Law is available at here.

protects all personal information of natural persons processed in respect of "commercial transactions" (explained below) that are (i) processed in Malaysia and (ii) processed outside Malaysia where the data are intended to be further processed in Malaysia. The Malaysian Law does not apply, however, to personal information processed by federal and state governments.

In Brief. *The Malaysian Law restricts cross-border transfers and requires registration. It does not require the appointment of a DPO or data security breach notification.*

Special Characteristics

Data Protection Authority. The Personal Data Protection Commissioner, located within Ministry of Information, Communication and Culture ("Malaysian DPA"), is responsible for regulating and overseeing compliance with the Malaysian Law.[58]

Application of the Law. A "commercial transaction" is defined as "any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a Credit Reporting Business carried out by a Credit Reporting Agency under the Credit Reporting Agencies Act 2009." Given this definition, there has been much speculation about whether this law would apply to the processing of human resources data. While no official guidance has been issue, all indications are that the Malaysian Law does apply to human resources data.

Cross-Border Transfers. Organizations may only transfer personal information to countries outside Malaysia that have been approved by the Minister unless an exception applies. The exceptions largely mirror those found in many European laws such as:

- the individual has consented to the transfer;
- the transfer is necessary to perform a contract with or at the request of an individual;
- the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising, or defending legal rights;

58. The website address of the Malaysian DPA is here.

- the transfer is necessary in order to protect the vital interests of the individual; or
- the organization has taken all reasonable precautions and exercised all due diligence to ensure that the personal information will not be processed in any manner which, if the data were processed in Malaysia, would be a contravention of the Act.

Approved countries have not been published by the Malaysian DPA.

Registration. Data Users (mainly licensed organizations) from the following sectors are required to register: communications, banking and financial institutions, insurance, health, tourism and hospitalities, transportation, education, direct selling, services (such as legal, audit, accountancy, engineering or architecture, retail or wholesale dealing as defined under the Control Supplies Act 1961), private employment agencies, real estate, and utilities.

NEW ZEALAND

New Zealand was the first country in the region to enact a data protection law. The Privacy Act 1993 ("New Zealand Law"), which regulates the processing of all personal information of natural persons by both the public and private sectors, is also the first and only law in Asia to be recognized by the EU as providing an adequate level of protection for personal data transferred from the EU/EEA.[59] This adequacy determination was issued after New Zealand amended its law in 2010 to establish a mechanism for controlling the transfer of personal information outside of New Zealand in cases where the information has been routed through New Zealand to circumvent the privacy laws of the country from where the information originated.

In Brief. *The New Zealand Law requires the appointment of a DPO but does not restrict cross-border transfers or require registration. There are no mandatory requirements to provide notice in the event of a data security breach; however, such notice is recommended by the DPA.*

59. The New Zealand Law is available here.

Special Characteristics

Data Protection Authority. The Office of the Privacy Commissioner (DPA) regulates and administers the New Zealand Law.[60]

Data Protection Officer. A DPO must be appointed regardless of the size of the Agency. One DPO per agency is required.

Data Security Breach Notification. There are no mandatory notification obligations; however, the DPA has issued voluntary guidelines that recommend notice be provided to individuals and/or the DPA in the event of a security breach that presents a risk of harm to the individuals whose personal information are involved in the breach. Necessity to provide notice should be assessed on a case-by-case basis.

THE PHILIPPINES

Philippine President Benigno Aquino III signed the Data Privacy Act of 2012 ("Philippine Law") into law Aug. 15, 2012. While the law entered into force Sept. 8, 2012, the Implementing Rules and Regulations (Rules) were not issued until September 2016. [61] The Rules introduced significant changes to or expanded upon the legal requirements set forth in the Philippine Law, particularly with respect to third-party disclosures, security, registration, data breach notification, and internal policy requirements. In addition, the exemption for outsourcing was narrowed.

In December 2016, the Philippine National Privacy Commission issued additional rules for managing and reporting data breaches. These rules require, among other things, the creation of a data breach response team and outline the elements to be contained in a security incident management policy, preventive measures to be taken, and the internal documentation and DPA notification requirements.

In Brief. *The Philippine Law imposes the same rules for both domestic and international (cross-border) transfers and requires the appointment of a DPO and data security breach notification. The Philippine Law does not require registration. In addition, the Philippine Law contains an exemption for outsourcing providers.*

60. The website address of the New Zealand DPA is here.
61. The Philippine Law is available here and the Implementing Rules and Regulations are available here.

Special Characteristics

Data Protection Authority. The National Privacy Commission ("Philippines DPA"), established in March 2016, is responsible for administering, implementing, and monitoring compliance with the Philippine Act, as well as investigating and settling complaints. Located within the Department of Information and Communications Technology (DICT), the Philippines DPA does not have the power to directly impose penalties; it can only recommend prosecution and penalties to the Department of Justice.[62]

Application of the Law. The Philippine Law applies to the processing of all personal information of individuals by public and private sector organizations with some important exceptions. For example, personal information that is collected from residents of foreign jurisdictions in accordance with the laws (e.g., data privacy laws) of those jurisdictions and that is being processed in the Philippines is excluded; however, data controllers and processors remain subject to the requirements of implementing data security measures under the Philippine Law and Rules. This exception is relevant for companies that outsource their processing activities to the Philippines. As a result, outsourcing providers in the Philippines will not need to comply with the Philippine Law's requirements (except for data security) for information collected as part of their outsourcing operations relating to personal information received from outside the Philippines.

In addition, the Philippine Law also applies to processing that is done or engaged in by an organization with links to the Philippines that uses equipment located in the Philippines, maintains an office, branch, or agency in the Philippines for processing personal data, has entered into a contract in the Philippines, provides its parent or affiliate with access to the personal data, carries on business in the Philippines, or collects or holds personal data in the Philippines. The Philippine Law also applies to processing outside the Philippines if the processing relates to personal information about a Philippine citizen or a resident. This last provision seeking to extend the obligations of the law based on the citizenship of the individuals is very unusual in data protection laws.

Cross-Border Transfers/Transfers to Third Parties. Organizations are responsible for personal information under their control or custody, including information that has been transferred to a third

62. The website of the National Privacy Commission is here.

party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. Organizations are accountable for complying with the requirements of the Philippine Law and must use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party. This approach to domestic and international transfers is similar to the approaches found in Canadian and Japanese laws that are based on the concept of accountability.

Data Protection Officer. As part of the required organizational security measures, controllers and processors must designate an individual or individuals who will function as data protection officer (DPO) or compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security. In March 2017, the Philippines DPA issued advisory guidelines on the designation of data protection and compliance officers. The guidelines set forth detailed rules in a number of areas including the data protection officer's duties and responsibilities, appointment status, and degree of independence, and the controller's and processor's obligations vis-a-vis their data protection and compliance officers.

Data Portability. Where personal information is processed by electronic means and in a structured and commonly used format, the individual has the right to obtain from the controller a copy of the data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the individual. The Commission may specify the electronic format, as well as the technical standards, modalities and procedures for their transfer.

Data Security Breach Notification. The controller must notify the Philippines DPA and affected individuals within seventy-two hours when the controller or the processor has knowledge or a reasonable belief that a personal data breach requiring notification has occurred. Notification of a data breach is required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the controller or the Philippines DPA believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected Individual. These rules require, among other things, the creation of a data breach response team and outline the elements to be contained in a security incident management policy, preventive measures to be taken, and the internal documentation and DPA notification requirements.

Registration. Personal information processing systems operating in the country that involve accessing or requiring sensitive personal information of at least one thousand individuals must be registered, including the personal information processing systems of contractors, and their personnel, entering into contracts with government agencies. (Prior to the issuance of the Rules, the registration requirement only applied to the public sector.) Automated processing operations where the processing becomes the sole basis of decision making that would significantly affect the individual must be notified to the Commission.

SINGAPORE

Singapore's Personal Data Protection Act 2012 ("Singapore Law") came into force in January 2013.[63] The Singapore Law governs the collection, use, and disclosure of personal information by private sector organizations. It also prohibits the sending of certain marketing messages to Singapore telephone numbers, including mobile, fixed-line, residential, and business numbers registered with the Do Not Call (DNC) Registry. The Singapore Law was implemented in phases, with the DNC Registry provisions coming into force in January 2014 and the data protection rules coming into force in July 2014.

The following summarizes the special characteristics of data protection provisions only. It does not address the DNC Registry provisions contained in the Singapore Law.

In Brief. *The Singapore Law restricts cross-border transfers and requires the appointment of a DPO. Data security breach notification and registration are not required. The Singapore Law provides special exemptions for outsourcing providers and the collection, use, and disclosure of business contact information*.

Special Characteristics

Data Protection Authority. The Personal Data Protection Commission ("Singapore DPA") is responsible for enforcement of the Singapore Law.[64]

Application of the Law. The Singapore Law applies to all private sector organizations incorporated or having a physical presence in

63. The Singapore Law is available here.
64. The website address of the Singapore DPA is here.

Singapore; however, service providers that process on behalf of other organizations are exempted from all but the security and data retention provisions. All personal information of natural persons is protected with some important exceptions. For example, business contact information – defined as an individual's name, position name or title, business telephone number, address, email or fax number, and other similar information – is exempted from the provisions pertaining to the collection, use, and disclosure of personal information.

Cross-Border Transfers. Transferring organizations are required to take appropriate steps to determine whether, and ensure that, the recipient outside Singapore is bound by legally enforceable obligations to provide the transferred information with a comparable standard of protection. To satisfy these requirements, consent, a transfer contract, binding corporate rules, or another exception under the Singapore Law must apply.

Data Breach Notification. There is no express obligation under the Singapore Law on any entities to give notice in the event of a data security breach. However, in May 2015, the Singapore DPA issued a Guide to Managing Data Breaches, which recommends that individuals whose personal information has been compromised be notified immediately if a data breach involves sensitive Personal Data. The Singapore DPA should be notified of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals.

Data Protection Officer. Organizations must designate one or more data protection officer(s) responsible for ensuring the organization's compliance with the Singapore Law.

SOUTH KOREA

The Data Protection Act ("PIPA or Korean Law"), which took effect in September 2011, regulates public and private sector processing of personal information of natural persons.[65] PIPA serves as the umbrella privacy law in Korea; however, there are various sector-specific laws such as the Act on the Promotion of IT Network Use and Information Protection ("the Network Act"), the Use and Protection of Credit Information Act, the Electronic Financial Transactions Act, and the Use and Protection of Location Information Act that also regulate privacy and cybersecurity. The Network Act, enacted before PIPA, regulates the processing of personal information in

65. The Korean Act is available in Korean here.

the context of services provided by telecommunications service providers and commercial website operators. While the privacy-related provisions are similar to PIPA, the Network Act regulates issues not covered by PIPA, such as spam.

In Brief. *The Korean Law restricts cross-border transfers and requires the appointment of a DPO and data security breach notification. It also imposes extensive obligations in such areas as notice, consent, and data security. Registration is not required, however.*

Special Characteristics

Data Protection Authority. The Ministry of the Interior and Safety (MOIS) is the authority responsible for enforcing the Korean Law.[66]

Notice and Consent. Prior notice and express consent are required to collect, use, and transfer personal information. The notice must separately detail collection and use of personal information, third-party disclosures (including any cross-border disclosures), processing for promotional or marketing purposes, processing of sensitive information or particular identification data (such as resident registration number and passport number), disclosures to third-party outsourcing service providers, and transfers in connection with a merger or acquisition. The individual must consent separately to each item. The uses that do not require consent must be distinguished from those that do require consent.

Cross-Border Transfers. If an organization intends to provide personal information to a third party across the national border, it must give notice and obtain a specific consent to authorize the cross-border transfer.

Data Protection Officer. Organizations must appoint a DPO with specified responsibilities.

Data Security. The Korean Law and subsequent guidance issued by the regulatory authorities also impose significant data security obligations. For example, organizations are required to encrypt particular identification data, passwords, and biometric data when such data are in transit or at rest. If personal information is no longer necessary after the retention period has expired or when the purposes of the processing have been accomplished, the organization must, without delay, destroy the personal information unless any other law or regulation requires otherwise.

66. The website address for MOIS is here (in Korean) and here (in English).

Data Security Breach Notification. When becoming aware of a leak of personal information, organizations must, without delay, notify the relevant individuals, prepare measures to minimize possible damages, and, when the volume of affected data meets or exceeds a threshold set by executive order (i.e., in the case of a leak involving 1,000 or more individuals), notify the regulatory authorities concerned or certain designated specialist institutions.

TAIWAN

Taiwan's Personal Data Protection Act ("Taiwanese Law") entered into effect in October 2012.[67] The Taiwanese Law replaces the 1995 Computer Processed Personal Data Protection Act that regulated computerized personal information in specific sectors such as financial, telecommunication, and insurance. The Taiwanese Law now provides protection to personal information of natural persons across all public and private entities and across all sectors. Because of public concerns about the rules pertaining to the use of sensitive personal information and personal information collected prior to the enactment of the new law, the government delayed implementation of these provisions. However, in December 2015, the legislature enacted amendments, which took effect in March 2016, to address these concerns as well as fine tune some of the existing rules for consent and legal grounds for processing.

In Brief. *The Taiwanese Law requires data security breach notification but does not restrict cross-border transfers or require the appointment of a DPO or registration of databases*.

Special Characteristics

Data Protection Authority. The Ministry of Justice has overall responsibility for the Taiwanese Law; however, the individual government agencies that regulate specific industry sectors are authorized to regulate compliance by organizations under their regulatory jurisdiction.[68]

Cross-Border Transfers. There are no restrictions imposed on cross-border transfers; however, the central competent authority for a

67. The Taiwanese Law is available in English here.
68. The website address for the Ministry of Justice is here.

specific industry may restrict cross-border transfers in certain circumstances, such as if the recipient country does not yet have proper laws and regulations to protect personal information so that the rights and interests of the individual may be damaged or personal information is indirectly transferred to a third country to evade the Taiwanese Law.

Data Security Breach Notification. Individuals must be notified when their personal information has been stolen, divulged, or altered without authorization, or infringed upon in any way.

TURKMENISTAN

In March 2017, Turkmenistan enacted a privacy law ("Turkmenistan Law") that regulates the processing of personal information by both the public and private sectors. [69] The Turkmenistan Law, which takes effect on July 1, 2017, is largely a consent-based regime. In particular, written consent is required to collect, use, and disclose personal information unless one of the limited exceptions applies.

In Brief. *The Turkmenistan Law restricts cross-border transfers but does not require registration, the appointment of a DPO, or data breach notification*.

Special Characteristics

Data Protection Authority. The Turkmenistan Law authorizes the government to establish a privacy regulator to work with the State Prosecutor's Office to oversee and enforce the law. Access and Correction Individuals have the right to access and correct their personal information. Organizations must respond to access and correction requests within one working day.

Access and Correction Individuals have the right to access and correct their personal information. Organizations must respond to access and correction requests within one working day.

Cross-Border. Transfers Personal information may not be transferred to countries that do not provide protection unless one of the limited exceptions applies, such as written consent or where necessary to protect the life or health of the individual.

69. The Turkmenistan Law is available here.

ASIA (EAST, CENTRAL, AND SOUTH) AND THE PACIFIC MANDATORY REQUIREMENTS				
COUNTRIES WITH PRIVACY LAWS	**REGISTRATION**	**DPO[70]**	**CROSS-BORDER LIMITATIONS**	**DATA SECURITY BREACH NOTIFICATION[71]**
14	**4**	**5**	**11**	**5**
Australia	No	No	**Yes**	**Yes**
Hong Kong	No	No	No	No
India	No	No	**Yes**	No
Japan	No	**Yes**	**Yes**	**Yes**
Kazakhstan	No	No	**Yes**	No
Kyrgyzstan	**Yes**	No	**Yes**	No
Macao	**Yes**	No	**Yes**	No
Malaysia	**Yes**	No	**Yes**	No
New Zealand	No	**Yes**	No	No
Philippines	**Yes**	**Yes**	**Yes**	**Yes**
Singapore	No	**Yes**	**Yes**	No
South Korea	No	**Yes**	**Yes**	**Yes**
Taiwan	No	No	No	**Yes**
Turkmenistan	No	No	**Yes**	No

70. In some jurisdictions, the appointment of a Data Privacy Officer (DPO) may exempt the organization from its registration obligations.
71. This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

Miriam Wugmeister
Christine Lyon
Cynthia Rich

Morrison & Foerster LLP

May 2019

PRIVACY LAWS IN AFRICA AND THE NEAR EAST

INTRODUCTION

In Africa and the Near East, twenty-two jurisdictions have comprehensive privacy laws: Angola, Bahrain, Benin, Burkina Faso, Cape Verde, Chad, Cote d'Ivoire—also known as the Ivory Coast—Equatorial Guinea, Gabon, Ghana, Israel, Lesotho, Madagascar, Mali, Mauritius, Morocco, Qatar, Senegal, Seychelles, South Africa, Tunisia, and the United Arab Emirates (Dubai International Financial Centre and Abu Dhabi Global Market). Uganda reportedly has enacted a privacy law, but it is not yet published in the official gazette. In addition, there are indications that countries such as Kenya, Niger, Tanzania, and Zimbabwe in Africa and Saudi Arabia in the Near East may be close to adopting legislation.

Several of the existing regimes in the region are still in their formative stages, in large part because the regulators are either not yet in place or have been recently appointed and/or have insufficient funding; however, in some of the countries with the more established privacy regimes, the regulators have been stepping up their enforcement efforts.

OVERVIEW

While most of the core data protection principles and requirements are embodied in the laws of Africa and the Near East, specific requirements, particularly with respect to registration, cross-border transfers, data security, data breach notification, and the appointment of a data protection officer (DPO) vary widely from each other and from laws in other regions of the world.

At the end of the summary, there is a tally of the countries in the region to show at a glance the ones with mandatory cross-border, DPO, data security breach notification, and registration obligations. As the chart shows, all but one jurisdiction require registration; all but three jurisdictions contain cross-border limitations; slightly more than one-fourth require data security breach notification, and only three require the appointment of a DPO.

ANGOLA

The Personal Data Law, Law no. 22/11 ("Angolan Law"), which became effective in June 2011, regulates the processing of all personal information of natural persons by both the public and private sectors.[72]

In Brief. *The Angolan Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration, and imposes some additional security requirements*. *However, there is no obligation to appoint a DPO or give notice in the event of a data security breach. There are, however, breach notification obligations under an electronic communications law as discussed below*.

Special Characteristics

Data Protection Authority. The Angolan Law provides for the establishment of the Data Protection Agency ("Angola DPA"). The Angola DPA will be responsible for supervising and monitoring compliance with data protection laws and regulations. However, the Angola DPA has not yet been established.[73]

Cross-Border Transfers. The transfer of personal information to countries that do not ensure an adequate level of protection requires, as a rule, the individual's unambiguous, explicit and written consent, and prior authorization from the Angola DPA.

Data Security. In addition to the usual data security obligations, there are specific rules for processing sensitive information. Moreover, the Angolan Law specifies that the processing systems must separate data concerning health or sex life, including genetic data, and other personal information. In addition, where such data are transmitted via a network, in specific cases the Angola DPA may require the data to be "encoded."

Data Security Breach Notification. While there are no breach notification requirements under the Angolan Law, there are, however, breach notification obligations under the Law on Electronic Communications and Information Society Services, which require operators in the electronic communications sector to give notice in the event of a data security breach. An "operator" is an undertaking that provides or is authorized to provide a communications network or electronic communications services. In particular, where there is a violation of

72. The Angolan Law is available here.
73. The website for the Angolan DPA is not available.

security measures that, intentionally or recklessly, results in the destruction, loss, whole or partial alteration, or unauthorized access to personal information transmitted, stored, retained, or otherwise processed in connection with the provision of electronic communications services in Angola, the operator must, without undue delay, notify the DPA and the INACOM (Regulatory Authority for Electronic Communications in Angola; Instituto Angolano das Comunicac¸o˜es).

Registration. The Angolan Law requires that all personal information to be processed be registered for all purposes prior to the beginning of processing, unless an exemption applies. Certain types of processing require prior DPA authorization. For example, the processing of sensitive information and personal credit video surveillance data, as well as transfers to countries that do not provide an adequate level of protection, require DPA authorization. The registration process is not yet operative, pending the establishment of the DPA.

BAHRAIN

The Personal Data Protection Law ("Bahrain Law"), enacted in July 2018, regulates the automated and manual processing of all personal information of natural persons by both the public and private sectors. The Bahrain Law goes into effect on August 1, 2019.[74]

In Brief. *The Bahrain Law restricts cross-border transfers to countries that do not provide adequate protection and requires registration or the appointment of a Data Protection Officer. There is no obligation to give notice in the event of a data security breach.*

Special Characteristics

Data Protection Authority. The Bahrain Law provides for the establishment of the Personal Data Protection Authority ("Bahrain DPA") to oversee compliance with the Bahrain Law.

Cross-Border Transfer. Organizations may transfer personal information to countries outside Bahrain that have been identified by the Bahrain DPA as provided adequate protection. To transfer to inadequate countries, DPA authorization, express written consent or another legal basis such as contractual necessity or vital interests is required.

74. The Bahrain Law is available here.

Data Protection Officer. The appointment of a DPO is not required; however, the appointment of a DPO does eliminate the need to register with the DPA. The Bahrain Law does authorize the Bahrain DPA to designate special categories of controllers that are required to appoint a DPO.

Legal Bases for Processing. A legal basis is required to process personal data. Legal bases include express written consent, balance of interests, contractual necessity, legal requirement, or vital interests.

Registration. Organizations must register their processing with the Bahrain DPA unless they have appointed a DPO. Registration of processing for HR-related purposes is not required. Internal records of all processing must also be maintained by the DPO or the controller.

BENIN

Law no. 2009-09 on the Protection of Personal Data ("Benin Law"), enacted in 2009, regulates the processing of all personal information of natural persons by both the public and private sectors.[75]

In Brief. *The Benin Law restricts cross-border transfers to countries that do not provide adequate protection and requires registration. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO; however, if a DPO is appointed, registration is not required*.

Special Characteristics

Data Protection Authority. The Commission Nationale de l'Informatique et des Liberte´s ("Benin DPA"), an independent administrative authority, is charged with overseeing compliance with the Benin Law.[76]

Cross-Border Transfer. Organizations may only transfer personal information to countries outside Benin that provide an adequate level of protection. DPA authorization is required for all processing of personal information that includes transfers to countries outside Benin, clauses or internal rules.

75. The Benin Law is available here.
76. The website for the Benin DPA is here.

Data Protection Officer. There is no requirement to appoint a DPO; however, registration is not required if a DPO is appointed to maintain a registry of the organization's processing activities.

Registration. Organizations must register the processing with the Benin DPA for all data and all purposes except where such processing is carried out for certain purposes, such as general accounting, personnel payroll management, or supplier management purposes. Registration is not required if the organization appoints a person to maintain a registry of the processing activities. In addition, organizations must register all video surveillance systems and, in some cases, obtain DPA authorization. DPA authorization is also required to process biometric data, health data, and national ID numbers.

BURKINA FASO

Law no. 010-2004 on the Protection of Personal Data ("Burkina Faso Law"), enacted in 2004, regulates the processing of all personal information of natural persons by both the public and private sectors.[77]

In Brief. *Databases must be registered with the DPA, and transfers of personal information to countries outside Burkina Faso are only permitted where they are carried out in a manner that ensures an equivalent level of protection. There are also special security rules for certain types of health care data. However, there is no obligation to appoint a DPO or give notice in the event of a data security breach.*

Special Characteristics

Data Protection Authority. The Commission de l'Informatique et des Liberte´s ("Burkina Faso DPA") is responsible for enforcement of the Burkina Faso Law.[78]

Cross-Border Transfers. Transfers of personal information to countries outside Burkina Faso are only permitted where the transfers are carried out in a manner that ensures an equivalent level of protection for the personal information. Specific DPA authorization is not required for cross-border transfers, but such transfers must be included in the prior registration with the Burkina Faso DPA.

77. The Burkina Faso Law is available here.
78. The website for the Burkina Faso DPA is here.

Data Security. Nominative data disclosed by health care professionals through automated processing must be coded before they are transmitted, except where the processing of data is associated with drug monitoring studies (pharmacovigilance) or research agreements concluded in the context of national and international cooperative studies, or when the distinct features of the research require it.

Registration. Organizations must register all processing of personal information with the Burkina Faso DPA prior to commencement of the processing. The recipients or categories of recipients to whom personal information is or may be disclosed must be included in the registration with the Burkina Faso DPA.

CAPE VERDE

The Law on Protection of Personal Data, enacted in 2001 and amended in 2013 ("Cape Verde Law"), regulates persons by both the public and private sectors.[79]

In Brief. *The Cape Verde Law restricts cross-border transfers of personal information, requires registration of data processing, and imposes some additional data security obligations; however, there is no obligation to appoint a DPO or give notice in the event of a data security breach*.

Special Characteristics

Data Protection Authority. The Comissao Nacional de Proteccao de Dados ("Cape Verde DPA"), an independent administrative authority working with the National Assembly of Cape Verde, is responsible for the supervision of the protection of the personal information of individuals and for monitoring compliance with the terms of the Cape Verde Law. The Cape Verde DPA was established in April 2015.[80]

Cross-Border Transfers. Personal information may only be transferred to a country that ensures an adequate level of protection unless an exception applies. Such exceptions include: the individual's consent, contractual necessity, legal requirement, and vital interests. Transfers to countries that do not ensure an adequate level of protection require prior DPA authorization. International transfers based on the individual's consent also require prior DPA authorization.

79. The Cape Verde Law is available here.
80. The website for the Cape Verde DPA is here.

Data Security. In addition to the usual data security obligations, there are specific rules for processing sensitive information. Moreover, where such data are transmitted via a network, in specific cases the Cape Verde DPA may require the data to be "encoded."

Registration. Organizations must register all personal information for all purposes prior to the beginning of the processing, unless an exemption applies. In addition, processing of certain types of data such as sensitive personal information requires prior DPA authorization.

CHAD

Act 007/PR/2015 Regarding The Protection Of Personal Data ("Chad Law"), enacted in 2015, regulates the processing of all personal information of natural persons by both the public and private sectors.[81]

In Brief. *The Chad Law restricts cross-border transfers of personal information and requires data breach notification and registration of data processing. There is no obligation to appoint a DPO; however, if a DPO is appointed, then the organization may be exempt from registration.*

Special Characteristics

Data Protection Authority. The Chad Law provides for the creation of the Agence Nationale de Securite Informatique et de Certification Electronique ("Chad DPA"), which is responsible for enforcing compliance with the Chad Law. The Chad DPA is not yet established.

Cross-Border Transfers. Personal information may not be transferred to a country outside the Central African Economic and Monetary Community (CEMAC) and the Economic Community of Central African States (CEEAC) unless that country ensures an adequate level of data protection. The six members of CEMAC are: Gabon, Cameroon, the Central African Republic (CAR), Chad, the Republic of the Congo, and Equatorial Guinea. The 10 members of CEEAC are: Angola, Burundi, Cameroon, Central African Republic, Congo, Democratic Congo, Gabon, Equatorial Guinea, Sao Tome & Principe, and Chad. If the transfer is to a country that is not considered adequate, the individual must consent to the transfer or another exemption, such as contractual necessity, must apply. Organizations must notify the DPA

81. The Chad Law is available here.

in advance of such transfers. The DPA may also authorize transfers to a third country where the organization has in place appropriate contractual clauses.

Data Security Breach Notification. Notice must be provided to individuals and the Chad DPA whenever there is any breach of security that affects personal information.

Registration. Organizations must register all personal information for all purposes, prior to the beginning of the processing, unless an exemption applies. In addition, processing of certain types of data, such as sensitive personal information, genetic and biometric data, and national ID numbers requires prior DPA authorization.

COTE D'IVOIRE

The Law 2013-450 on Protection of Personal Data ("Cote d'Ivoire Law"), enacted in August 2013, regulates the processing of all personal information of natural persons by both the public and private sectors.[82]

In Brief. *The Cote d'Ivoire Law restricts cross-border transfers, requires registration, imposes additional security measures and establishes the right to be forgotten. Data security breach notification is not required, and the appointment of a DPO is voluntary*.

Special Characteristics

Data Protection Authority. Enforcement of the Cote D'Ivoire Law and the other missions of the DPA are conferred on the Telecommunications/ICT Regulatory Body of Cote d'Ivoire ("Cote d'Ivoire DPA"), an independent administrative authority.[83]

Cross-Border Transfers. Organizations may only transfer personal information to a "third country" that provides an equivalent level of protection. Prior DPA authorization is required for such transfers. The Cote D'Ivoire Law defines a "third country" as any country outside the Economic Community of West African States (ECOWAS). The 15 ECOWAS member states currently are: Benin, Burkina Faso, Cape Verde, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, the Togolese Republic, and

82. The Cote d'Ivoire Law is available in French here, and in English here.
83. The website for the Cote d'Ivoire DPA is here.

Cote d'Ivoire. There are no limitations on the transfer of personal information to other ECOWAS member states.

Data Protection Officer. The appointment of a DPO is voluntary; however, the appointment of a DPO relieves the organization of general registration requirements but not of the requirement to obtain prior authorization for the transfers to third countries.

Data Security. The Cote D'Ivoire Law specifies in greater detail than other laws the technical and organizational measures required. In particular, there are 10 specific obligations imposed on organizations, such as an organization must:

- guarantee that it is possible to know and verify the identity of any third parties to whom the data are transmitted by transmission installations;
- guarantee that it is possible to know and verify, *a posteriori*, the identity of persons who have had access to the information system; the nature of the data that have been entered, modified, altered, copied, erased, or read in the system; and the time at which they were manipulated;
- prevent the unauthorized reading, copying, modification, alteration, or deletion of data when the data are communicated or transported in storage media; and
- prevent the use of processing systems for money laundering or terrorist financing.

Organizations must also prepare an annual report for the Cote d'Ivoire DPA on their compliance with the security measures required under the law.

Registration. Organizations must register all processing of personal information with the Cote d'Ivoire DPA prior to the commencement of processing, unless a DPO has been appointed or another exception applies. Prior authorization is required for certain types of processing of personal information. Registrations may be submitted to the Cote d'Ivoire DPA by e-mail, postal mail or in any other form that allows a receipt to be issued. The Cote d'Ivoire DPA will make a decision in response to the registration/request for prior authorization within one month from the day it is received (the one-month period may be extended once upon the reasoned decision of the Cote d'Ivoire DPA); the data organization may begin the processing once it has received such receipt. The absence of a receipt from the Cote d'Ivoire

DPA means that the Cote d'Ivoire DPA has rejected the registration/ request for prior authorization. The data controller may appeal such decision in the competent court.

Right to Be Forgotten. Where an organization has authorized a third party to publish personal information, the organization is deemed responsible for the publication and must take all appropriate measures to implement the digital "right to be forgotten" and the right to have one's personal information deleted. The organization must put in place appropriate mechanisms to ensure the respect of the "right to be forgotten" in a digital context.

EQUATORIAL GUINEA

Law No. 1/2016, Law on Personal Data Protection ("Equatorial Guinea Law"), enacted in 2016, regulates the processing of all personal information of citizens by both the public and private sectors.[84]

In Brief. *The Equatorial Guinea Law restricts cross-border transfers of personal information and requires registration of data processing. There is no obligation to appoint a DPO or provide notification in the event of a data security breach.*

Special Characteristics

Data Protection Authority. The Equatorial Guinea Law provides for the creation of the Personal Data Protection Governing Authority ("Equatorial Guinea DPA"), which is responsible for enforcing compliance with the Equatorial Guinea Law. The Equatorial Guinea DPA is not yet established.

Cross-Border Transfers. Organizations may not transfer any processed personal information to countries that that fail to provide a legally equivalent level of protection, unless the transfer has been previously authorized by the Equatorial Guinea DPA or an exception such as consent or contractual necessity applies.

Registration. Organizations must register their processing of personal information with the Equatorial Guinea DPA.

84. The Equatorial Guinea Law is available here.

GABON

Law no. 001/2011 on the Protection of Personal Data ("Gabon Law"), enacted in 2011, regulates the processing of all personal information of natural persons by both the public and private sectors.[85]

In Brief. *The Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes additional security requirements and health rules. The appointment of a DPO is not required, but the appointment of one may relieve the organization of some, but not all, of its registration obligations. There is no obligation to give notice in the event of a data security breach or appoint a DPO.*

Special Characteristics

Data Protection Authority. The National Commission for the Protection of Personal Data ("Gabon DPA"), an independent administrative authority, is responsible for enforcement. The Gabon DPA was established in November 2012; however, there is no website established yet.

Cross-Border Transfers. Organizations may not transfer personal information to countries that do not provide a sufficient level of the protection, unless an exception applies. Exceptions include consent, contractual necessity, vital interests, and the establishment of legal claims. If none of the exceptions apply, the organization may apply to the Gabon DPA for authorization, particularly where the transfer relies on the use of contractual clauses or internal rules. The Gabon DPA will publish a list of countries that provide sufficient protection for personal information.

Data Protection Officer. There is no obligation to appoint a DPO; however, the appointment of a DPO exempts the organization from registration requirements but only where the processing does not involve cross-border transfers. The appointment of a DPO must be notified to the Gabon DPA and must be brought to the attention of employee representative bodies (e.g., works councils or labor unions). The DPO may not be sanctioned by his/her employer as a result of performing his/ her duties. If the DPO encounters difficulties while performing his/her duties, he/she must apply to the DPA. In cases of where the DPO does not carry out his required duties, the DPO may be discharged after consultation with the Gabon DPA.

85. The Gabon Law is available in French here.

Data Security. Like the Cote d'Ivoire Law, the Gabon Law also imposes detailed security requirements. However, the Gabon requirements are potentially more onerous because organizations must:

- guarantee that unauthorized persons cannot access automated processing systems or the personal information contained therein;
- guarantee that any third parties to which personal information is or can be transferred, identified, and verified;
- guarantee that it is possible to identify and verify any access to and entry of data into the system after such access has taken place, as well as what data were accessed or entered, at what time, and by whom;
- prevent unauthorized access to the premises and equipment used for the processing of personal information;
- prevent storage media from being read, copied, modified, destroyed, or moved by unauthorized persons;
- prevent the unauthorized entry of any data into the information system, as well as any unauthorized knowledge, modification, or deletion of personal information;
- prevent systems from being used by unauthorized persons with the aid of data transmission equipment;
- prevent the unauthorized reading, copying, modification, or deletion of any personal information or storage media containing personal information while in transit;
- save personal information (make backup copies); and
- refresh and, if necessary, convert data for permanent storage.

Health professionals may transfer personal information they use within the framework of the authorized processing of personal information. Where such data permit the identification of individuals, they must be encrypted before they are transmitted, unless the data are associated with pharmacovigilance studies or research protocols carried out in the context of cooperative national or international studies or where necessitated by the specificity of the research. Personal information transferred to another country in the context of health research must be encrypted, unless the processing and transfer is in compliance with all the requirements for the lawful processing of personal information.

Registration. Organizations must register all processing with the Gabon DPA, unless a DPO has been appointed or an exception applies. Authorization is required for certain types of processing, such as the processing of sensitive information.

Special Health Rules. The publication of the results of processing of personal information for health research purposes must not, under any circumstances, permit the direct or indirect identification of individuals. The person responsible for the research must ensure that the processing respects the purposes for which the information was collected.

Data from medical files retained by health professionals and health insurance systems to carry out their functions cannot be communicated for purposes of statistical evaluation or analysis of medical treatment and prevention practices unless (i) the data are aggregated or organized in such a way that the individuals cannot be identified, or (ii) a specific authorization from the Gabon DPA is obtained. Exceptions to these requirements may only be authorized by the Gabon DPA and, in such cases, may not include the last name, first name, or national ID number of individuals. The results of the processing of such data must not, under any circumstances, be published in a form that permits the direct or indirect identification of individuals.

GHANA

The Data Protection Act (Act 843) ("Ghana Law"), enacted in May 2012, regulates the processing of all personal information of natural persons by both public and private sector organizations. The Ghana Law is one of the few data protection laws around the world that contains a carve-out for outsourcing. In particular, the Ghana Law states that, when personal information of foreign individuals is to be sent to Ghana for processing, the information must be processed in compliance with the data protection legislation of the foreign jurisdiction of the individual.[86]

In Brief. *The Ghana Law requires data security breach notification and registration. The appointment of a DPO is voluntary, and there are no restrictions imposed on cross-border transfers.*

86. The Ghana Law is available here.

Special Characteristics

Data Protection Authority. The Data Protection Commission ("Ghana DPA"), established in November 2014, is responsible for enforcement of the Ghana Law. The Ghana DPA is governed by a board consisting of representatives from different government agencies, industries and academia. It is unusual to have industry officials sit on the governing board.[87]

Data Protection Officer. The appointment of a DPO is voluntary. The Ghana Law provides for the DPA to establish qualifications criteria for DPOs and states that organizations should not appoint someone as a DPO unless he or she satisfies such criteria.

Data Security Breach Notification. Ghana was the first African country to include a breach notification obligation in its law. Under the Ghana Law, an organization, or the third party that processes personal information under the authority of the organization, must provide notice to the Ghana DPA and the affected individuals where there are reasonable grounds to believe that the personal information has been accessed or acquired by an unauthorized person. The organization must take steps to ensure the restoration of the integrity of the information system.

Registration. Organizations must register all processing of personal information with the Ghana DPA. The processing of personal information without a registration is prohibited. The recipients and countries to which personal information is intended to be transferred must be listed in the organization's database registration. The registration process opened in May 2015, and data controllers were given until July 31, 2015, to register with the Ghana DPA. Failure to register is an offense under the Ghana Law.

ISRAEL

The Protection of Privacy Law 5471-1981 ("Israeli Law"), enacted in 1981, regulates the processing of all personal information of natural persons by both the public and private sectors. Israel is the first and only country in the region to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/European Economic Area. In April 2017, the Israeli Parliament approved new privacy

87. The website for the Ghana DPA is here.

and data security regulations that impose additional obligations in a variety of areas, ranging from breach notification to physical maintenance of IT infrastructure. The regulations took effect in March 2018.

In Brief. *The Israeli Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration, and imposes detailed security requirements. Effective March 2018, owners of Intermediate and High Security Databases are required to report any data breaches to the DPA. While there is no obligation to appoint a DPO, there is an obligation on certain companies to appoint a Security Officer.*

Special Characteristics

Data Protection Authority. The Privacy Protection Authority (previously, until October 2017, the Israeli Law, Information and Technology Authority (ILITA)) ("Israeli DPA"), established in the Ministry of Justice, is responsible for enforcement of the Israeli Law.

Cross-Border Transfers. To transfer to third parties outside Israel, consent or another legal basis is required unless the transfer is to affiliates that are under the corporate control of the Israeli company. Prior authorization of cross-border transfers is not required.

Data Breach Notification. Effective May 2018, owners of Intermediate and High Security Databases must immediately report to the Israeli DPA any data breaches, as well as any measures they are taking in response to such incidents. The Israeli DPA may, after consultation with the Israel National Cyber Bureau, direct the database owner to provide notice to any individual whose personal information may have been compromised.

Data Security. The Israeli Law sets forth comprehensive security rules that include specific requirements for outsourcing activities. In addition, organizations with five or more databases that require registration, banks, insurance companies and companies, engaged in ranking or evaluating credit ratings must appoint a security officer. The identity of the security officer must be reported to the Israeli DPA.

New security regulations took effect in March 2018. Databases are classified into four categories: Individual-Managed Databases, Basic Security Databases, Intermediate Security Databases, and High Security Databases. Classification is determined primarily by the number of individuals who have access to the database, the number of individuals whose personal information is contained in the database, and the

types and the sensitivity of the information that the database contains. The regulations impose the fewest obligations on Individual-Managed Databases and the most obligations on High Security Databases. The following are some of the new requirements:

- **Specification manual and security procedures**. Each database owner must draft and annually update a specification manual that describes his or her database's contents and objectives, processing mechanisms, cross-border transfer practices, and third-party access, as well as a document, binding on all the owner's employees, outlining the security practices applicable to the database.
- **Data minimization**. Each database owner must annually evaluate whether his or her database contains more information than is necessary to achieve the objectives set forth in the database's specification manual.
- **Risk assessment/penetration testing**. Each owner of a High Security Database must conduct a comprehensive risk assessment with respect to and penetration testing of such database at least once every 18 months.
- **Authentication and Monitoring**. For Intermediate and High Security Databases, access must be authenticated by means of a physical token and automatically monitored by a system that identifies the user accessing the database, the time and date of access, and the information retrieved and/or processed.
- **Security Officer**. The regulations expand on the current requirement under the Israeli Law that certain companies retain a qualified Security Officer. The regulations impose seniority standards and conflict-of-interest rules specifying, among other things, that the Security Officer must be directly subordinate to the individual manager or owner of the database.

Registration. Databases that fall into specific categories (e.g., databases containing personal information on more than 10,000 people or databases containing sensitive information) must be registered with the Israeli DPA.

MADAGASCAR

Law no. 2014-038 on the Protection of Personal Data ("Madagascar Law"), enacted in January 2015, regulates the processing of personal information of natural persons by both public and private sector organizations.[88]

In Brief. *The Madagascar Law restricts cross-border transfers to countries that do not provide adequate protection. It also requires registration and the appointment of a DPO. However, there is no obligation to give notice in the event of a data security breach.*

Special Characteristics

Data Protection Authority. The Madagascar Law provides for the establishment of the Malagasy Commission on Informatics and Liberty ("Malagasy DPA"), an independent regulator, which is charged with enforcement of the law. The Malagasy DPA is not yet established.

Cross-Border Transfers. Organizations may not transfer personal information to countries that do not provide adequate protection unless the Malagasy DPA authorizes the transfer based on, for example, contractual clauses or internal rules that provide sufficient guarantees of adequate protection. Alternatively, such transfers can take place where an exception applies, such as consent, contractual necessity, vital interests, or a legal requirement. The Madagascar Law also prohibits subsequent transfers except with the approval of the organization responsible for the original processing and the Malagasy DPA.

Data Protection Officer. A DPO must be appointed. The appointment of a DPO relieves the organization of its registration obligations, except in cases where the processing requires DPA authorization. The Malagasy DPA will maintain a list of the designated DPOs.

Registration. The processing of personal information must be registered with the Malagasy DPA. The processing of personal information that poses special risks to individuals requires DPA authorization before such processing can begin.

88. The Madagascar Law is available here.

MALI

Law no. 2013/015 on the Protection of Personal Data ("Mali Law") was adopted in May 2013. It regulates the processing of all personal information of legal and natural persons by both the public and private sectors. The Mali Law is unusual because it protects the personal information of both individuals and companies and, as discussed below, there are no explicit rules regarding consent.[89]

In Brief. *The Mali Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration, and imposes some additional security requirements. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.*

Special Characteristics

Data Protection Authority. The Authority for the Protection of Personal Data ("Mali DPA") became operational in March 2016.[90]

Consent. There are no explicit rules regarding consent. The Mali Law only states that notice must be provided and the natural or legal person must be advised that they have the right to refuse to be included in a personal data file. Moreover, both legal and natural persons have a general right to oppose the processing of their personal information on legitimate grounds. In addition, the processing of sensitive personal information is prohibited unless one of the narrow exceptions applies; consent is not one of the legal bases listed.

Cross-Border Transfers. Organizations may transfer personal information to a third country where the third country to which the information is transferred provides an adequate level of protection for personal information, as determined by the Mali DPA. Transfers of personal information to a third country that does not provide an adequate level of protection may be authorized by the DPA where both the transfer and the processing by the recipient guarantee an adequate level of protection for privacy, notably by the use of contractual clauses or internal rules.

Registration. Organizations must register all processing operations for a specific purpose with the Mali DPA.

89. The Mali Law is available here.
90. The website for the Mali DPA is here.

MAURITIUS

The Data Protection Act 2004 ("Mauritius Law") regulates the processing of all personal information of natural persons by both the public and private sectors.[91]

In Brief. *The Mauritius Law restricts cross-border transfers to countries that do not provide adequate protection and requires registration. However, there is no obligation to appoint a DPO or give notice in the event of a data security breach. The DPA has issued voluntary data security and data security breach notifications guidelines, however.*

Special Characteristics

Data Protection Authority. The Data Protection Commissioner ("Mauritius DPA") is responsible for monitoring and enforcing compliance with the Mauritius Law. While the Mauritius DPA operates under the aegis of the prime minister's office, the Mauritius DPA was guaranteed functional independence after an amendment was enacted in 2009.[92]

Cross-Border Transfers. Written authorization from the Mauritius DPA is required for all transfers of personal information to countries outside Mauritius. In addition, personal information may only be transferred to countries that do not provide an adequate level of protection where the individual has consented to the transfer or another exception applies. Other exceptions include contractual necessity and DPA-approved contracts or binding corporate rules.

Data Security. The Mauritius DPA has published detailed guidelines on security practices and privacy impact assessments.

Data Security Breach Notification. There is no mandatory obligation to give notice in the event of a data security breach under the Mauritius Law; however, the Mauritius DPA has issued Guidelines for Handling Privacy Breaches, which recommend that organizations provide notice to individuals and/or the Mauritius DPA in the event of a security breach that presents a risk of harm to the individuals whose personal information is involved in the breach.

Registration. All organizations must register with the Mauritius DPA prior to the commencement of the processing of any personal information.

---

91. The Mauritius Law is available here.
92. The website for the Mauritius DPA is here.

MOROCCO

Law no. 09-08 on the Protection of Individuals in Relation to the Processing of Personal Data ("Moroccan Law"), which took effect in 2009, regulates the processing of all personal information of natural persons by both the public and private sectors.[93]

In Brief. *The Moroccan Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration, and imposes some additional security requirements. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.*

Special Characteristics

Data Protection Authority. The National Supervisory Authority ("Moroccan DPA") is responsible for supervising compliance with the Moroccan Law.[94]

Cross-Border Transfers. Personal information may only be transferred to a foreign country that does not ensure an adequate level of protection where an exception applies, such as vital interests or contractual necessity, or where there are DPA-authorized contractual clauses or binding corporate rules (BCRs) in place. All jurisdictions that have been found by the EU as proving adequate protection are similarly recognized by the Morocco.

Data Security. There are specific requirements on organizations that process sensitive information, including health data, as well as provisions related to encryption and the supervision of service providers. According to the Moroccan DPA, organizations have the obligation to ensure through contractual means and compliance audits that their service providers comply with security requirements. The Moroccan DPA has issued template language that organizations may use in their contracts with data processors.

Registration. Organizations must register all partially or wholly automatic processing of personal information with the Moroccan DPA prior to the commencement of processing, unless an exception applies. In addition to registration, prior authorization must be obtained for certain types of processing, such as the processing of sensitive information including genetic, health, and criminal data.

93. The Moroccan Law is available in French here.
94. The website for the Moroccan DPA is here.

QATAR

Law no. (13) of 2016 on the Protection of Personal Data ("Qatar Law") was enacted in December 2016 and became effective in January 2017. The Qatar Law applies to personal information that is electronically processed or obtained, collected, or extracted by any other means in preparation for electronic processing by controllers, processors, and website operators. Personal information is defined as data of a person whose identity is determined or can be reasonably determined, whether by these data or by collecting them with any other data.

Prior to the enactment of the national law, only organizations licensed to operate in the Qatar Financial Centre (QFC) were subject to data privacy rules. The QFC is a financial and business center located in Doha that was established by the government of Qatar in 2005 to attract international financial services and multinational corporations to grow and develop the market for financial services in the region. The QFC has no physical boundaries. It is an onshore jurisdiction established in the State of Qatar, which operates alongside of, but separate from, the civil and commercial laws of the state.[95]

In Brief. *The Qatar Law restricts cross-border transfers in cases where the processing would violate the Qatar Law or harm the privacy of individuals. Notification is required in the event of a data security breach and a permit is required to process sensitive personal information. Registration and the appointment of a DPO, however, are not required.*

Special Characteristics

Data Protection Authority. The Minister of Transport and Communications ("Qatar DPA") is responsible for issuing the decrees necessary to implement the provisions of the Qatar Law.[96]

Collection and Use. A controller must not process any personal information, unless the controller obtains the individual's consent or where the processing is necessary for the legitimate purpose of the controller or the other party to whom the data will be sent or an exception applies. Sensitive personal information may only be processed after obtaining a permit from the competent department according to the procedures and controls to be set forth in a ministerial decree.

95. The Qatar Law is available in Arabic here.
96. The website for the Qatar DPA is here.

Cross-Border Transfers. A controller must not make any decision or take an action that may reduce the cross-border flow of personal information unless the processing of the information violates the provisions of the Qatar Law or would cause a serious harm to the personal information or the privacy of an individual.

Data Security Breach Notification. The controller must notify an individual and the competent department of any breach if it may cause serious harm to the personal information privacy of said individual. The processor must notify the controller of any breach or any threat to an individual's personal information as soon as the processor becomes aware of the breach or threat. The Qatar Law does not prescribe what information must be contained in the notice to affected individuals and when notice must be provided.

SENEGAL

Act no. 2008-12 on the Protection of Personal Data ("Senegalese Law"), which took effect in 2008, regulates the processing of all personal information of natural persons by both the public and private sectors.[97]

In Brief. *The Senegalese Law restricts cross-border transfers to countries that do not provide adequate protection and requires registration. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.*

Special Characteristics

Data Protection Authority. The Commission for the Protection of Personal Data ("Senegalese DPA") is responsible for enforcement of the Senegalese Law.[98]

Cross-Border Transfers. Organizations may only transfer personal information to a third country if that third country provides a sufficient level of protection. However, organizations may transfer personal information to a third country without adequate protection if the transfer is occasional and not massive and if the individual has provided his/her express consent to the transfer, or if another exception applies, such as

97. The Senegalese Law is available here.
98. The website for the Senegalese DPA is here.

contractual necessity or vital interests. The Senegalese DPA may authorize a transfer or group of transfers to a third country without adequate protection where the organization provides sufficient guarantees.

Registration. Organizations must register all automatic processing of personal information with the Senegalese DPA unless an exception applies. In addition to registration, certain processing is subject to DPA authorization, such as where the information is transferred to countries that do not provide adequate protection or where certain types of data such as sensitive information is processed.

SEYCHELLES

The Data Protection Act, 2003 (No. 9 of 2003) ("Seychelles Law") regulates the processing of all personal information of natural persons. The Seychelles Law was enacted in 2002 but has never entered into force.[99]

In Brief. *The Seychelles Law requires registration with the DPA. There are no restrictions on cross-border transfers set forth in the law; however, the DPA has the authority to prohibit such transfers as explained below. There is no requirement to appoint a DPO or give notice in the event of a data security breach.*

Special Characteristics

Data Protection Authority. The Seychelles Law provides for the establishment of a Data Protection Commissioner ("Seychelles DPA"); however, there is no indication that one has been established.

Cross-Border Transfers. The Seychelles DPA has the power to prohibit cross-border transfers if it believes such transfers will violate the data protection principles under the act.

Registration. Processing must be registered with the Seychelles DPA.

SOUTH AFRICA

South Africa's Protection of Personal Information Act ("South African Law") was published in the official gazette Nov. 26, 2013; however, it will only commence on a date to be proclaimed by the president. Organizations will have one year from the date of commencement to comply with

99. The Seychelles Law is available here.

the South African Law. The South African Law regulates the processing of all personal information of natural and legal persons by both the public and private sectors.[100]

In Brief. *The South African Law restricts cross-border transfers to countries that do not provide adequate protection. It also requires data security breach notification, the appointment of a DPO, and registration.*

Special Characteristics

Data Protection Authority. The Information Regulator ("South African DPA"), established in December 2016, will be responsible for enforcement of the law when the South African Law enters into force.[101]

Cross-Border Transfers. Organizations may not transfer personal information to a third party in a foreign country unless the individual consents to the transfer; the recipient is subject to a law, a contract, or BCRs that provide an adequate level of protection; or another exception applies. Prior DPA authorization is required to transfer sensitive personal information or personal information of children to a third party in a foreign country that does not provide an adequate level of protection, unless a code of conduct is applicable.

Data Protection Officer. A DPO must be appointed. Each organization must also ensure that it appoints as many deputy DPOs as necessary to fulfill its access obligations under the law. Deputy DPOs will have the same powers and duties as the DPO.

Data Security Breach Notification. Organizations must notify the South African DPA and the individual when there are reasonable grounds to believe that personal information has been accessed or acquired by any unauthorized person. Notice must be given as soon as reasonably possible after the discovery of the beach.

Registration. The South African Law imposes limited registration obligations, requiring organizations to notify the South African DPA about any processing that is subject to authorization requirements under the law. Authorization is required prior to processing information such as unique identifiers, sensitive information, and children's information transferred to a third party in a foreign country that does not provide an adequate level of protection.

---

100. The South African Law is available here.
101. The website for the South African DPA is here.

TUNISIA

The Organic Law no. 2004-63 on Personal Data Protection ("Tunisian Law"), which took effect in 2004, regulates the processing of all personal information of natural persons by both the public and private sectors.[102]

In Brief. *The Tunisian Law restricts cross-border transfers to countries that do not provide adequate protection. It also requires registration and the appointment of a DPO.*

Special Characteristics

Data Protection Authority. The National Authority for Protection of Personal Data ("Tunisian DPA") is responsible for enforcement of the Tunisian Law.[103]

Cross-Border Transfers. Personal information may not be transferred to countries outside Tunisia unless that country ensures an adequate level of protection. Moreover, transfers outside Tunisia must be approved by the Tunisian DPA.

Data Protection Officer. Organizations must list on the registration/ notification forms the name of the DPO. The DPO must have Tunisian nationality, reside in Tunisia, and have a clean criminal record.

Registration. The Tunisian Law provides for two kinds of registrations: notifications that are applicable to all kinds of data and authorizations that are applicable to sensitive data. The processing of sensitive information may not begin without an affirmative authorization from the Tunisian DPA. Prior authorization is required for the cross-border transfer of personal information to countries outside Tunisia.

UNITED ARAB EMIRATES

Private sector organizations located in the Dubai International Financial Center (DIFC), a 110-acre area within the city of Dubai, are subject to the DIFC Data Protection Law (DIFC Law), which was enacted in 2007 and amended in 2012. The DIFC is a federal financial free zone established in 2004 for the conduct of financial services. It has its own civil and commercials laws, court system and judges, and financial regulator, separate

102. The Tunisian Law is available in French here, and in English here.
103. The website for the Tunisian DPA is here.

from the United Arab Emirates. The DIFC Law regulates the processing of all personal information by controllers.[104]

In addition, private sector organizations that are licensed to operate in the Abu Dhabi Global Market (ADGM), a financial free zone in Abu Dhabi, are subject to the ADGM Data Protection Regulations (ADGM Regulations). The ADGM Regulations, issued in 2015 and amended in 2018, regulate the processing of personal information by controllers and processors.

In Brief. *The DIFC Law and the ADGM Regulations restrict cross-border transfers to countries that do not provide adequate protection, require registration, and impose data security breach notification obligations. There is no requirement to appoint a DPO.*

Special Characteristics

Data Protection Authority. The Commissioner of Data Protection ("DIFC DPA") is responsible for enforcement of the DIFC Law[105]; the ADGM Registration Authority ("ADGM DPA") is responsible for enforcement of the ADGM Regulation.

Cross-Border Transfers. Personal information may not be transferred to countries outside the DIFC or ADGM that do not provide an adequate level of protection unless the individual has consented in writing, the DPA has authorized the transfer, or another exception such as contractual necessity or vital interests applies.

Data Security Breach Notification. In the event of an unauthorized intrusion, whether physical, electronic, or otherwise, to any personal information database, organizations in the DIFC and ADGM must notify the DPA. Notice to individuals is not legally required.

Registration. Organizations must file a notification with the DIFC and ADGM DPAs concerning any processing of sensitive personal information and any transfers of personal information to a recipient in a territory outside the DIFC or the ADGM that is not subject to laws and regulations that ensure an adequate level of protection.

104. The DIFC Law is available here. The ADGM 2015 Regulations are available here; the ADGM 2018 amendments are available here .
105. The website for the DIFC DPA is available here. The website for the ADGM DPA is available here.

AFRICA/NEAR EAST MANDATORY REQUIREMENTS				
COUNTRIES WITH PRIVACY LAWS	**REGISTRATION**	**DPO[106]**	**CROSS-BORDER LIMITATIONS**	**DATA SECURITY BREACH NOTIFICATION[107]**
22	**21**	**3**	**19**	**7**
Angola	**Yes**	No	**Yes**	No
Bahrain	**Yes**	No (voluntary)	**Yes**	No
Benin	**Yes**	No	**Yes**	No
Burkina Faso	**Yes**	No	**Yes**	No
Cape Verde	**Yes**	No	**Yes**	No
Chad	**Yes**	No (voluntary)	**Yes**	**Yes**
Cote D'Ivoire	**Yes**	No (voluntary)	**Yes**	No
Equatorial Guinea	**Yes**	No	**Yes**	No
Gabon	**Yes**	No	**Yes**	No
Ghana	**Yes**	No	No	**Yes**
Israel	**Yes**	No	**Yes**	**Yes**
Lesotho	**Yes**	No (voluntary)	**Yes**	**Yes**
Madagascar	**Yes**	**Yes**	**Yes**	No
Mali	**Yes**	No	**Yes**	No
Mauritius	**Yes**	No	**Yes**	No (recommended)
Morocco	**Yes**	No	**Yes**	No
Qatar	No	No	No	**Yes**
Senegal	**Yes**	No	**Yes**	No
Seychelles	**Yes**	No	No	No
South Africa[108]	**Yes**	**Yes**	**Yes**	**Yes**
Tunisia	**Yes**	**Yes**	**Yes**	No
UAE/DIFC	**Yes**	No	**Yes**	**Yes**

106. In some jurisdictions, the appointment of a Data Privacy Officer (DPO) may exempt the organization from its registration obligations.
107. This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.
108. South Africa's Protection of Personal Information Act, 2013 was signed into law by the President in November 2013; however, the law does not take effect until the President proclaims a commencement date. It is unknown when the President will set a commencement date.

Miriam Wugmeister
Christine Lyon
Cynthia Rich

Morrison & Foerster LLP

May 2019

PRIVACY LAWS IN EUROPE AND EURASIA (NON-EEA)

INTRODUCTION

With the implementation of the European General Data Protection Regulation (GDPR) in May 2018, attention of the business community has been focused on changes to the privacy rules in the 28 Member States of the European Union (as well as Switzerland and the other members of the European Economic Area or EEA). However, these changes are likely to have a ripple effect on existing privacy laws in the seventeen jurisdictions in Europe and Eurasia that are not part of the EU/EEA: Albania, Andorra, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Georgia, Kosovo, Macedonia, Moldova, Monaco, Montenegro, Russia, San Marino, Serbia, Turkey, and Ukraine. In fact, efforts are already underway in some countries to modify existing laws to conform to the GDPR. For example, Serbia enacted a new privacy law in November 2018 that closely mirrors the GDPR.

At present, though, most of the laws in these jurisdictions contain the basic elements found under EU Member State laws, but some also have unique elements not found in other laws in the region or within the EEA.

OVERVIEW

All of the countries in the region that have enacted comprehensive data privacy laws impose a common set of data protection obligations such as notice, consent, access and correction, security, cross-border transfer restrictions, and registration obligations. However, there is wider variation among the jurisdictions with respect to Data Protection Officer (DPO) and data security breach notification. The following summary, therefore, focuses on the major differences among these data privacy laws. Where applicable, the responsible enforcement authority and any other noteworthy characteristics specific to each jurisdiction are also highlighted.

At the end of the summary, there is a tally of the countries in the region to show at a glance the ones with mandatory cross-border, DPO, data

security breach notification, and registration obligations. As the chart shows, all but one of the 17 laws in this region impose restrictions on cross-border transfers; all but two require database registration similar to the requirements under European laws; and about one quarter require that individuals and/or the regulator be notified in the event of a data security breach.

ALBANIA

The Protection of Personal Data Law ("Albanian Law") which became effective in 2008 and was amended mostly recently in 2014, regulates the processing of all personal information of natural persons by both the public and private sectors.[109]

In Brief. *The Albanian Law requires database registration, imposes data protection officer (DPO) and special data security obligations, and restricts cross-border transfers to countries that do not provide adequate protection*. *However, there are no data breach notification requirements*.

Special Characteristics

Data Protection Authority. The Commissioner for Information Rights and Protection of Personal Data ("Albanian DPA"), an independent administrative authority, is charged with overseeing compliance with the Albanian Law. It carries out online and onsite inspections on its own initiative and in response to complaints and issues fines, most commonly in cases where organizations fail to implement its recommendations or orders.[110]

Access and Correction. Access and correction requests must be responded to within 30 days.

Cross-Border Transfers. There are no restrictions on cross-border transfer of personal information to recipients in countries that provide an adequate level of data protection. Albania has recognized all EU/EEA countries, signatories to the 1981 Council of Europe Convention for "Protection of Individuals with regard to Automatic Processing of Personal Data", and countries recognized by the European Commission as providing adequate protection. To transfer personal information to a country that does not provide an adequate level of protection, DPA authorization is required or an exception under the law

109. The Albanian Law is available here.
110. The website for the Albanian DPA is here.

must apply. Exceptions include consent, contractual necessity, vital interests, or legal requirement.

Data Protection/Security Officer. Large data controllers (with six or more persons engaged in data processing) must authorize in writing one or more persons responsible for internal data security supervision. One of the people appointed will serve as the contact person, registered with the Commissioner. Small data controllers (with less than six persons engaged in data processing) may, but are not required to, authorize in writing, one or more persons responsible for the internal security supervision.

Data Security. Different organizational and technical data security measures are provided by law, depending on whether the controller is large or small. For example, small controllers must carry out a risk assessment procedure as a minimum standard measure of data security. Large controllers must apply and maintain an information security management system (SMSI). SMSI is based on the identification, assessment and mitigation of risks threatening personal information security while taking in consideration (i) the information technology and communication system used to process personal information, (ii) all manual forms of processing personal information and (iii) the physical security of premises and the security of the personnel, electronic and movable equipment. The risk assessment and treatment are part of the mandatory Information Security Policy of the Controller. Large controllers must carry out information security audits at least once per year and provide security training to employees. In addition, there are encryption requirements in connection with transfers of sensitive information and equipment used to process information through cloud computing platforms.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirement, legitimate interests, or vital interests.

Registration. The Albanian Law requires that controllers notify the Albanian DPA about all categories of personal information they process for all purposes unless one of the limited exemptions applies. However, even when a notification exemption applies, minimum information on the data processing activities must be provided such as name and address of controller, categories and purposes of processed information and categories of recipients. Depending on the category of information, the controller must either register the processing or obtain an authorization from the Albanian DPA prior to processing.

ANDORRA

The Protection of Personal Data Law ("Andorran Law"), which became effective in 2004, regulates public and private sector processing of all personal information of natural persons, except where the information relates to their business, professional or commercial activities. Andorra is regarded as providing an adequate level of protection for personal information transferred from the EU/EEA.[111]

In Brief. *The Andorran Law requires database registration and the appointment of a DPO and restricts cross-border transfers to countries that do not provide adequate protection. In addition, the period of time within which organizations must respond to access requests is exceedingly short and there is no provision for processing personal information on the basis of legitimate interests. However, there are no special security and data breach notification requirements.*

Special Characteristics

Data Protection Authority. The Andorran Agency for Data Protection ("Andorran DPA"), an independent public authority, is responsible for overseeing compliance with the Andorran Law.[112]

Access and Correction. Organizations must respond to access requests within five working days and correction requests within one month.

Cross-Border Transfers. Personal data may not be transferred to third countries that do not provide an equivalent level of protection unless consent or another of one of the limited exceptions such as contractual obligations, vital interests or legal requirements applies. Countries that provide an equivalent level of data protection are the EU Member States and countries found by the European Commission or the Andorran DPA to provide equivalent protection.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirement, or vital interests.

Registration. Controllers must register their databases with the Andorran DPA and update their registration records whenever there is a change in the information listed.

---

111. The Andorran Law is available here.
112. The website for the Andorran DPA is here.

ARMENIA

The Law on Personal Data ("Armenian Law"), which became effective in 2015, regulates the processing of all personal information of natural persons by both the public and private sectors.[113]

In Brief. *The Armenian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security and breach notification obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short and there are limited legal bases provided for the collection and use of personal information. However, there is no DPO obligation.*

Special Characteristics

Data Protection Authority. The State Body for the Protection of Personal Data Processing ("Armenian DPA") is responsible for enforcement of the law.[114]

Access and Correction. The Armenian Law does not specify a time period for responding to access requests. Corrections should be carried out (or refused) within five days after receiving the written request.

Cross-Border Transfers. Personal data may be transferred cross border either with the consent of the individual or where the transfer is necessary to carry out processing previously consented to by the individual. In addition, DPA authorization is required to transfer to those countries that are not on the Armenian DPA's approved list of countries that provide adequate protection. A transfer permit is required in such cases. The Armenian DPA must also approve the organization's contractual clauses governing the transfer.

Data Breach Notification. The data controller must make a public announcement without delay and notify the police and the Armenian DPA when a data security breach occurs.

Data Security. Encryption measures are required to protect information systems containing personal information from loss, unauthorized access, illegal use and destruction, and illegal copying and disclosure. The Armenian Law also provides for the government to set security

113. The Armenian Law is available here.
114. There is no website for the Armenian DPA. Information about the Armenian DPA is available here (in Armenian). The Ministry of Justice's website is here. The Armenian DPA decisions are available here.

standards for information systems, physical records of biometric data and personal data storage technologies other that electronic information systems.

Legal Basis for Collection and Use. Personal information may be processed only with the consent of the individual, where such processing is provided for or required by law, or where the data are publicly available.

Registration. The Armenian DPA has the right to require data controllers to notify it about the collection or processing of personal information; otherwise such notification is voluntary.

AZERBAIJAN

The Law on Personal Data ("Azerbaijani Law"), which became effective in 2010, regulates the processing of all personal information of natural persons by both the public and private sectors. The Azerbaijani Law differentiates personal information according to public and confidential categories. Public data are (i) data that are depersonalized or anonymized, (ii) data that are declared public by the individual or (iii) data that are included in an information system created for general use with the consent of the individual. A natural person's name, last name, and patronymic will always be considered to be public data.[115]

In Brief. *The Azerbaijani Law requires database registration, restricts cross-border transfers to countries that do not provide adequate data protection, and imposes special security obligations. In addition, the period of time within which organizations must respond to access and correction requests is exceedingly short and there are limited legal bases provided for the collection and use of personal information. However, there are no data breach notification or DPO obligations*.

Special Characteristics

Data Protection Authority. The State Register at the Ministry of Communications and Information Technologies ("Azerbaijani DPA") is responsible for registering information systems and ensuring compliance with the Azerbaijani Law.[116]

115. The Azerbaijani Law is available here.
116. The website for the Azerbaijani DPA is here.

Access and Correction. Organizations must respond to access and correction requests within seven days.

Cross-Border Transfers. Cross-border transfers are prohibited where: (i) such transfer creates a threat to the national security of the Azerbaijan Republic, or (ii) the laws of the countries to which the personal information is transferred do not provide the same level of protection as that provided by the Azerbaijani Laws. However, personal information can be transferred across the border to a country regardless of the level of legal protection of personal information where the individual expressly agrees to the transfer. In addition, although not expressly stated in the Azerbaijani Law, cross-border transfers are permitted where the transfer is necessary to protect the life or health of the individual.

DPA authorization is not required; however, information on such transfer and the categories of the personal information transferred must be provided to the Azerbaijani DPA at the time of the registration of the information system. The Azerbaijani DPA has stated informally that the cross-border transfer provisions apply to the transfer of databases (i.e. personal information of a significant number of individuals); transfers of personal information limited to one or several individuals across the border would likely trigger the rules for transfers to third parties, not the cross-border transfer rules.

Data Security. Data controllers and processors must implement organizational and technical measures to guarantee the security of personal information during its collection, use and disclosure (including cross-border transfer). They must determine the risks to personal information and based on such determination must continually improve the information system in order to neutralize possible risks. There are regulations that prescribe a long list of technical organizational safety requirements. Organizations must encrypt all transmitted records. The length of the encryption key used during the transfer may not be less than 256 bits. As is evident from the registration card for information systems approved by the Regulations on the Registration and Deregistration of Information Systems, organizations must have control and audit mechanisms for the collection and processing of personal information; however, the frequency of such audits and their substance have not been specified.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, legal requirement, or vital interests.

Registration. Information systems containing personal information must be registered with the State Register unless an exemption applies. The State Registry is maintained by the Data Computing Center at the Ministry of Communication and Information Technologies.

BELARUS

The Law on Information, Informatization and Protection of Information ("Belarusian Law"), which became effective in 2008, regulates the processing of all personal information of natural persons by both the public and private sectors.[117]

In Brief. *Under the Belarusian Law, consent is the only permissible basis on which to process (and transfer cross-border) personal information. In addition, the law imposes special security obligations; however, there are no registration, breach notification, or DPO obligations*.

Special Characteristics

Data Protection Authority. There is no DPA in Belarus akin to the DPAs found in other jurisdictions. The state authority that performs any data protection-related functions is the Operative Analytics Center of the President of the Republic of Belarus (OAC). However, to date, OAC competence is more technical in nature and does not include only data protection-related competence. For example, the OAC is empowered to certify IT systems, hardware and software data protection solutions, and regulate general IT and Internet relations.[118]

Access and Correction. The Belarusian Law does not specify a time period for responding to access requests and is silent on correction rights.

Cross-Border Transfers. There are no specific limitations on cross-border transfers. By general rule, each transfer, including cross-border transfers, requires the consent of the individual.

Data Protection/Security Officer. A special individual or department for security measures must be appointed.

Data Security. Data controllers must take effective measures to ensure security of personal information from the moment of receipt

117. The Belarusian Law is available here.
118. The website for the OAC is here.

until its destruction. Under the Belarusian Law and implementing regulations, this obligation includes various organizational and technical security measures. In particular, controllers must maintain a data protection system certified by the certification centers accredited by the OAC. Organizations must file annual reports on their security measures with the OAC by December 30th of each year. In addition, there are cryptographic regulations that define legal and organizational basics of technical and cryptographic measures of information security. Data controllers must comply with these regulations which among others things require that personal information be encrypted in transit. Regulation on Technical and Cryptographic Security of Information in the Republic of Belarus, approved by the Edict of the President of the Republic of Belarus N 196 On Certain Measures for Improving Information Security, 2013. Regulation On the Technical Security of Information and Regulation Onthe Technical and Cryptographic Protection of Information, both approved by the Order of Operative Analytics Center of the President of the Republic of Belarus of 30 August 2013 N 62.

Legal Basis for Collection and Use. Consent is required to process personal data. The Belarusian Law does not provide for any other legal bases such as contractual necessity, vital interests or legal requirements.

BOSNIA AND HERZEGOVINA

The Law on the Protection of Personal Data ("Bosnia and Herzegovina Law"), which became effective in 2006, regulates the processing of all personal information of natural persons by the public and private sectors.[119]

In Brief. *The Bosnia and Herzegovina Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security obligations. However, there are no data breach notification or DPO obligations.*

Special Characteristics

Data Protection Authority. The Personal Data Protection Agency ("Bosnia and Herzegovina DPA"), an independent administrative

119. The Bosnia and Herzegovina Law is available in English here; the amendment is available here.

organization, is responsible for enforcement of the Bosnia and Herzegovina Law.[120]

Access and Correction. Access requests must be responded to within 30 days; there is no specified time period for responding to correction requests.

Cross-Border Transfers. Personal data may not be transferred to another country that does not guarantee adequate safeguards for personal information that are equivalent to those under the Bosnia and Herzegovina Law, unless the prior consent of the individual has been obtained or another exception applies, such as contractual necessity or vital interests. Exceptionally, the Bosnia and Herzegovina DPA may authorize such transfers. Neither the Bosnia and Herzegovina Law nor the Bosnia and Herzegovina DPA provide a specific list of "adequate" countries, so the data controller is responsible for assessing whether the country to which personal data are transferred guarantees protections equivalent to those provided for under the Bosnia and Herzegovina Law.

Data Security. In addition to the general security obligations under the Bosnia and Herzegovina Law, regulations issued in 2009 set forth more detailed security requirements. In particular, the regulations require controllers and processors, among other things, to have a written security plan, data protection training for employees, and additional technical and organizational security measures for sensitive information such as encryption or equivalent "crypto-protection" when the data are in transit.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, legal requirements, or vital interests.

Registration. Data controllers must register all processing of personal data with the Bosnia and Herzegovina DPA prior to the establishment of the personal data filing system or any processing, unless one of the very narrow registration exemptions applies.

120. The website for the Bosnia and Herzegovina DPA is here.

GEORGIA

The Law on the Protection of Personal Data ("Georgian Law"), which went into effect in 2012 and was amended in 2014, regulates the processing of all personal information of natural persons by the public and private sectors.[121]

In Brief. *The Georgian Law requires database registration and restricts cross-border transfers to countries that do not provide adequate data protection. However, there are no data breach notification, DPO, or special security obligations.*

Special Characteristics

Data Protection Authority. The Personal Data Protection Inspector ("Georgian DPA"), an independent authority, is responsible for enforcing the Georgian Law.[122]

Access and Correction. Organizations must respond to access requests within 10 days and correction requests within 15 days.

Cross-Border Transfers. Transfers of personal information outside Georgia are permitted to countries that provide adequate data protection. The Georgia DPA issued a list of approved countries that include: the EEA countries, Australia, Albania, Andorra, Argentina, New Zealand, Bosnia and Herzegovina, Israel, Canada, Croatia, Macedonia, Moldova, Monaco, Montenegro, Serbia, Ukraine, and Uruguay. Where transfers are to jurisdictions that are not recognized as providing adequate protection, DPA-approved contracts are required.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration. Data controllers must register with the Georgian DPA prior to creation of filing systems and inclusion of new categories of data in those filing system.

121. The Georgian Law is available here.
122. The website for the Georgian DPA is here.

KOSOVO

The Law on the Protection of Personal Data ("Kosovo Law"), which went into effect 2010, regulates the processing of all personal information of natural persons by the public and private sectors.[123]

In Brief. *The Kosovo Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security obligations. However, there are no data breach notification or DPO obligations.*

Special Characteristics

Data Protection Authority. The National Agency for the Protection of Personal Data ("Kosovo DPA"), an independent agency, is responsible for enforcing the Kosovo Law.[124]

Access and Correction. Organizations must respond to access requests within 15 days and provide access within 30 days. They must comply with correction requests within 15 days.

Cross-Border Transfers. Personal Data may only be transferred to countries outside Kosovo that ensure an adequate level of data protection, unless one of the legal bases for data transfer applies (e.g., consent, contractual necessity, or vital interests). Adequate countries include the EEA countries and the other jurisdictions recognized by the EU as providing adequate protection. The Kosovo DPA must be notified about all transfers to inadequate countries; authorization is required for such transfers.

Data Security. Among other requirements, controllers and processors must have internal documentation that describes the personal information security measures that are in place. Sensitive personal information must be specifically protected and classified in order to prevent unauthorized access and use. Sensitive personal information that is transmitted over telecommunications networks will be considered suitably protected if the information is encrypted to ensure that it is rendered incomprehensible or unrecognizable.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

---

123. The Kosovo Law is available here.
124. The website for the Kosovo DPA is here.

Registration. Registration is required. The data controller must keep a record of all processing of personal information, called the "Filing System Catalogue", a copy of which must be filed with the Kosovo DPA prior to establishment of the filing system.

MACEDONIA

The Law on Personal Data Protection ("Macedonian Law"), which went into effect in February 2005, regulates the processing of all personal information of natural persons by the public and private sectors.[125]

In Brief. *The Macedonian Law requires database registration and the appointment of a DPO, restricts cross-border transfers to countries that do not provide adequate data protection, and imposes special security obligations. However, there is no data breach notification obligation.*

Special Characteristics

Data Protection Authority. The Directorate for Personal Data Protection ("Macedonia DPA"), an independent state authority, is responsible for enforcing the Macedonian Law.[126]

Access and Correction. Organizations must respond to access requests within 15 days and correction requests within 30 days.

Cross-Border Transfers. Personal information may only be transferred to countries that provide adequate protection (e.g., EEA countries). For all other transfers, one of the transfer exemptions must apply (e.g., consent, contractual necessity, or vital interests) or prior DPA authorization is required. In order to obtain approval of the Macedonian DPA, a written data transfer agreement must be in place between the controller and the recipient, preferably based on the EU Standard Contractual Clauses.

Data Protection Officer. The appointment of a DPO is required except where the controller a) has a collection of personal information that only refers to ten employees or less; or b) processes personal information of members of associations founded for political, philosophical, religious or trade-union purposes.

Data Security. There are special security rules that, together with the security provisions under the Macedonian Law, require, among other

125. The Macedonian Law is available in Macedonian here, and in English here.
126. The website for the Macedonian DPA is here.

things, adopting and implementing written security programs, carrying out risk assessments, conducting annual internal and triannual external audits, providing employee security training, encrypting data in transit, storing data on portable devices, and retaining back-up copies.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, and legal requirements.

Registration. All data must be registered by controllers for all purposes, unless one of the limited exemptions applies.

MOLDOVA

The Law on Personal Data Protection ("Moldovan Law"), which took effect in April 2012, regulates the processing of all personal information of natural persons by the public and private sectors.[127]

In Brief. *The Moldovan Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes data breach notification and special security obligations*. *However, there is no DPO obligation*.

Special Characteristics

Data Protection Authority. The National Centre for Personal Data Protection ("Moldovan DPA"), an independent agency, is responsible for enforcing the Moldovan Law.[128]

Access and Correction. Access and correction requests must be responded to without delay (no time period is specified).

Cross-Border Transfers. Personal data may not be transferred to countries outside Moldova, unless that country ensures an adequate level of data protection. If the proposed transfer is to a country that is not considered adequate, one of the transfer exceptions must apply, such as consent, contractual necessity, or vital interests. DPA authorization is also required in such cases.

Data Security. The Moldovan Law and implementing regulations prescribe detailed security requirements which include the need to maintain and annually reevaluate the organization's data security policy and

127. The Moldovan Law is available in Romanian here.
128. The website for the Moldovan DPA is here.

implement specific physical and electronic security measures, including encryption. Regular data security audits must be carried out. These audits must include an assessment of the organization, its security measures and use of communication partners and suppliers. The results of the security audit must be documented.

Data Security Breach Notification. All controllers must submit to the Moldovan DPA an annual report on any security incidents involving information systems during that year.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, and legal requirements.

Registration. Controllers and processors must register their processing for all purposes unless one of the limited exemptions applies.

MONACO

The Protection of Personal Data Act ("Monaco Law"), which took effect in December 1993, regulates the processing of personal data of natural persons by the public and private sectors.[129]

In Brief. *The Monaco Law requires database registration and the appointment of a DPO and restricts cross-border transfers to countries that do not provide adequate protection. However, there are no data breach notification or special security obligations*.

Special Characteristics

Data Protection Authority. The Personal Data Protection Supervisory Commission ("Monaco DPA") is responsible for enforcement compliance with the Monaco Law.[130]

Access and Correction. Access and correction requests must be responded to within one month.

Cross-Border Transfers. Personal information may not be transferred outside Monaco unless the recipient country provides an adequate level of data protection. Parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") are recognized as

129. The Monaco Law is available in French here, and in English here
130. The website for the Monaco DPA is here.

providing adequate data protection. Where the transfer is to a country which does not provide adequate data protection, one of the specified legal bases must apply such as consent, vital interests, or contractual necessity. In addition, the Monaco DPA may authorize transfers on the basis of appropriate contractual clauses.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration. Data controllers must register all automatic processing of personal information with the Monaco DPA unless one of the limited exceptions applies. Certain processing is also subject to Monaco DPA authorization (e.g., biometric data).

MONTENEGRO

The Personal Data Protection Law ("Montenegrin Law"), which took effect in 2012, regulates the processing of personal data of natural persons by the public and private sectors.[131]

In Brief. *The Montenegrin Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO and special security obligations. However, there is no data breach notification obligation.*

Special Characteristics

Data Protection Authority. The Personal Data Protection Agency ("Montenegrin DPA"), an independent regulatory authority, is responsible for enforcing the Montenegrin Law.[132]

Access and Correction. Organizations must respond to access and correction requests within 15 days.

Cross-Border Transfers. Personal data may be transferred from Montenegro to an EEA country or a country deemed adequate by the EU, or where the transfer is based on EU Standard Contractual Clauses. Alternatively, the transfer may take place where another legal basis applies such as consent, contractual necessity, or vital interests. Otherwise, DPA authorization is required.

131. The Montenegrin Law is available in Montenegrin here.
132. The website for the Montenegrin DPA is here.

Data Protection Officer. Where the data controller has 10 or more employees performing data protection activities, it must designate a person who will be responsible for the data protection matters immediately after establishing a personal data filing system.

Data Security. Detailed security requirements are set forth in the Regulation on the Form and Manner of Maintaining of Personal Data Filing System, covering areas such as the form, the manner of keeping data in personal data filing systems, the content of the records, the types of personal information contained in the filing system, the data retention periods, the manner of collection of personal information, and the transfer of data. For example, the Regulations require that sensitive information be kept separately, according to the type of data and that the legal basis on which the personal information is being processed is noted in the data filing system.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration. Prior to establishing a personal data filing system, the data controller must inform the Montenegrin DPA by submitting the notification containing all of the prescribed elements. Personal data filing systems required by law do not require registration.

RUSSIA

The Federal Law No. 152-FZ On Personal Data ("Russian Law"), which took effect in January 2007, regulates the processing of all personal information of natural persons by h the public and private sectors. The Russian Law was recently amended in 2014, imposing controversial data localization requirements.[133]

In Brief. *The Russian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO, data breach notification, special security, and data localization obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short and there is no provision for processing personal information on the basis of legitimate interests.*

133. The Russian Law is available in Russian here.

Special Characteristics

Data Protection Authority. The Federal Service for Supervision in the Field of Communication Information Technology and Mass Communications, commonly known as Roscomnadzor, ("Russian DPA") is responsible for enforcement of the Russian Law.[134]

Access and Correction. Organizations must respond to access requests within 30 days and correction and deletion requests within 10 days.

Cross-Border Transfers. Personal Data may only be transferred to a country that provides a sufficient level of protection. The countries recognized by the Russia DPA as providing adequate protection include: all of the signatories to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Armenia, Azerbaijan, Bosnia & Herzegovina, Georgia, Moldova, Montenegro, Macedonia, San Marino, Serbia, Turkey, Ukraine, Uruguay and the EEA Member States), Angola, Argentina, Australia, Benin, Canada, Cape Verde, Chile, Costa Rica, Gabon, Hong Kong, Israel, Kazakhstan, Malaysia, Mali, Mexico, Mongolia, Morocco, New Zealand, Peru, Qatar, Senegal, Singapore, South Africa, South Korea, Switzerland, and Tunisia.

Transfers to countries that do not provide adequate protection are permitted where there is a legal basis such as consent, contractual necessity, or vital interests. Prior DPA approval or authorization is not required; however, if the organization is subject to the registration requirements, it must indicate in its registration the countries to which it transfers the information.

Data Protection Officer. The appointment of an internal data protection officer is required.

Data Localization. Under the amended law, organizations that collect and process personal information of Russian citizens (in electronic and paper form) must store that information in Russia. Organizations must notify the Russian DPA of their server locations. The Russian DPA will maintain a register of violators and will block any infringing websites. These localization requirements only apply to deliberate activities to collect information from Russians.

134. The website for the Russian DPA is here.

Data Breach Notification. In the event of a data security breach, organizations must take measures to remedy the breach (or, if that is not possible, to destroy the affected data) within three days and then notify affected individuals about such measures. The Russia DPA must be notified (about rectification of the breach) only if it has issued a request to the organization to remedy the breach. The requirements to notify individuals about a security breach apply to any situation where an organization has processed the wrong data or there was any unauthorized processing of personal information. Such a breach may be detected by the organization itself or as a result of an access or correction request by the individual concerned.

Data Security. Organizations must take all reasonable organizational and technical measures to protect personal information, which include adopting internal data protection rules that are mandatory for all employees and conducting risk assessments, audits and oversight of compliance with the Russian Law. In addition, organizations must maintain special IT systems for protecting personal data (software and hardware measures) that comply with the technical requirements of the Russian

Federal Security Service (FSB) and the Federal

Service for Technical and Export Control (FSTEK), and in particular with the Order of FSTEK No. 21 dated February 18, 2013.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirements, or vital interests.

Registration. Organizations must notify the Russia DPA of their intent to process personal information, unless an exception applies. For example, registration is not required to process employee data or where personal information was obtained through an agreement between the organization and the individual concerned, and such information is not distributed or transferred to third parties without the consent of the individual; they are used by the organization solely for the purposes of performance of the agreement or for entering into new agreements with the individual in the future; Organizations must also register the location of databases that contain personal information of Russian citizens.

SAN MARINO

The Law Regulating the Collection of Personal Data ("San Marino Law"), which went into effect in 1995, regulates the processing of all personal information of natural and legal persons by the public and private sectors.[135]

In Brief. *The San Marino Law requires DPA authorization to process personal information unless one of the limited legal bases applies. There is no provision for processing personal information on the basis of consent (except in the case of sensitive information) or legitimate interests. DPA authorization is always required for cross-border transfers. However, there are no DPO, data breach notification, or special security obligations.*

Special Characteristics

Data Protection Authority. The Garante for the Protection of Confidentiality of Personal Data ("San Marino DPA") is responsible for enforcement of the San Marino Law. There is no website for the San Marino DPA.

Access and Correction. The San Marino Law does not prescribe a time frame to comply with access and correction requests.

Cross-Border Transfers. San Marino DPA authorization is required to transfer cross-border personal information of San Marino citizens or companies. The San Marino Law does not set out any specific requirements or conditions that must be met to obtain DPA authorizations for such cross-border transfers.

Legal Basis for Collection and Use. To collect and use personal information in a private data bank, prior San Marino DPA authorization is required unless an exception applies such as contractual necessity, legal requirement or the information is publicly available. The San Marino Law does not set out consent obligations for the use of personal information except where such information concerns political, union or religious opinions and activities. In such cases, express consent is required.

Registration. Prior San Marino DPA approval is required for the collection, processing and use of personal information by private owners of data banks unless an exception applies such as contractual necessity, legal requirement, the information is publicly available, or

135. The San Marino Law is available in Italian here.

the personal information is processed by a political, social or cultural organization and relates to the members of that organization.

SERBIA

The Law on Personal Data Protection ("Serbian Law"), which went into effect in 2009, protects all personal data of natural persons processed by the public and private sectors.[136] On November 21, 2018, a new Law on Personal Data Protection which mirrors the GDPR was adopted; the new Law will enter into force in July 2019.[137]

In Brief. *The current Serbian Law requires database registration and restricts cross-border transfers. In addition, the period of time within which organizations must respond to correction requests is exceedingly short. However, there are DPO, data breach notification, or special security obligations.*

Special Characteristics

Data Protection Authority. The Commissioner for Information of Public Importance and Personal Data Protection ("Serbian DPA") is responsible for enforcing the Serbian Law.[138]

Access and Correction. Organizations must respond to access requests within 30 days and correction and deletion requests within 10 days.

Cross-Border Transfers. Data can be transferred from Serbia to a country that is a signatory to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Data may be transferred to a state that is not a party to the Convention if such state has a regulation or a data transfer agreement in force which provides a level of data protection equivalent to that envisaged by the Convention. In cases of data transfers that do not provided an equivalent level of protection, DPA authorization is required.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

---

136. The Serbian Law is available here.
137. The text of the new Serbian law is available here.
138. The website for the Serbian DPA is here.

Registration. Controllers must register their processing with the Serbian DPA for all purposes. Very limited exceptions apply.

TURKEY

The Law on the Protection of Personal Data ("Turkish Law"), which was enacted in March 2016 and entered into full force in October 2016, regulates the processing of personal information of natural persons by individuals and private sector organizations.[139]

In Brief. *The Turkish Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, expansively defines and limits processing of sensitive information, and imposes breach notification and special security obligations. However, there is no DPO obligation.*

Special Characteristics

Data Protection Authority. The Turkish Data Protection Board ("Turkish DPA") is responsible for enforcement of the Turkish Law. Its powers include the ability to impose administrative sanctions for law violations.[140]

Cross-Border Transfers. To transfer personal information outside of Turkey, express consent of the individual must be provided unless one of the exceptions applies (e.g., contractual necessity, vital interests, legitimate interests, or legal requirement). In addition, the transfer of personal information may only be to countries that provide adequate data protection (the Turkish DPA will provide a list). If the transfer is to a country that does not provide adequate protection, there must be a contract in place between the parties and the Turkish DPA must authorize the transfer.

Data Breach Notification. Organizations must notify individuals and the Turkey "as soon as possible" if personal information is obtained by third parties "in an illegal manner."

139. The Turkish Law is available here.
140. The website for the Turkish DPA is here.

Data Security. The data controller must take every necessary technical and administrative precaution to prevent unlawful processing of and access to personal information and ensure the safeguarding of that information. In addition, the data controller must carry out the necessary internal inspections and audits to ensure compliance with the Turkish Law. If the personal information will be processed by a third party processor, the data controller will be jointly responsible for the necessary security measures.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as explicit consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration. The Turkish Law requires data controllers to register their processing activities before they begin processing. Exceptions may be specified by the Turkish DPA. The registration process is not yet in place; however, the Turkish DPA has issued for public comment draft regulations on the creation of a database registry. Once the public comments period ends in late June 2016, the regulations are expected to be finalized and published shortly after. The regulations should enter into force immediately upon publication.

Sensitive Information. The Turkish Law defines special categories of personal information (i.e., sensitive information) as information related to a person's racial and ethnic origins, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership with associations, foundations or trade unions, health or sexual life, criminal convictions, and biometric and genetic data related to security measures. Processing of this information is prohibited except with the explicit consent of the individual. However, such information - with the exception of health and sexual life – may be processed without explicit consent where such processing is envisaged under Turkish laws. Health and sexual information may be processed by persons or authorized institutions and organizations that are bound by confidentiality obligations, solely for the purpose of protecting public health, and providing preventive medicine, medical diagnosis, treatment and care, healthcare services and healthcare financial planning and management.

UKRAINE

The Law on the Protection of Personal Data ("Ukrainian Law"), which went into effect in 2011, regulates the processing of all personal data of natural persons by public and private sectors. The Ukrainian Law was amended in September 2015.[141]

In Brief. *The Ukrainian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO and special security obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short. However, there is no breach notification obligation.*

Special Characteristics

Data Protection Authority. The Ukrainian Parliament Commissioner for Human Rights ("Ukrainian DPA") is responsible for enforcement of the Law.[142]

Access and Correction. Organizations must respond to access and correction requests within 10 days.

Cross-Border Transfers. Personal data may be transferred to third countries that provide sufficient protection for personal information which include the EEA countries, signatories to the Council of Europe Convention and states on the DPA approved list (which is not yet adopted). Personal information can also be transferred to countries that do not provide adequate protection if a legal basis applies such as consent, contractual necessity, or vital interests. DPA authorization is not required; however, information regarding cross-border transfers of the personal information must be included in the original registration/ negotiation filed with DPA.

Data Protection Officer. Organizations must appoint a department or a person responsible for the protection of personal information during the processing of that information.

Data Security Breach Notification. There is no obligation for any entity to give notice in the event of a data security breach; however, the data controller must document or log violations in the course of data processing and develop a plan of action in case of any unauthorized access to personal information.

---

141. The Ukrainian Law is available here.
142. The website for the Ukrainian DPA is here.

Data Security. The Ukrainian Law and implementing regulations require organizations to, among other things, establish an internal security policy and implement specific security measures including employee training, data disposal measures, and documentation requirements involving access and control procedures.

Legal Basis for Collection and Use. To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration. Controllers must file a notification with the Ukrainian DPA about processing of certain categories of sensitive personal information such as health, biometrical and genetic data, geolocation, trade-union political or religious memberships, race ethnic or national origin, and criminal records.

EUROPE/ EURASIA (NON-EEA) MANDATORY REQUIREMENTS				
COUNTRIES WITH PRIVACY LAWS	**REGIS-TRATION**	**DPO[143]**	**CROSS-BORDER LIMIT-ATIONS**	**DATA SECURITY BREACH NOTIFI-CATION[144]**
17	**15**	**5**	**16**	**4**
Albania	**Yes**	**Yes**	**Yes**	No
Andorra	**Yes**	No	**Yes**	No
Armenia	No	No	**Yes**	**Yes**
Azerbaijan	**Yes**	No	**Yes**	No
Belarus	No	No	No	No
Bosnia and Herzegovina	**Yes**	No	**Yes**	No
Georgia	**Yes**	No	**Yes**	No
Kosovo	**Yes**	No	**Yes**	No
Macedonia	**Yes**	**Yes**	**Yes**	No
Moldova	**Yes**	No	**Yes**	**Yes**
Monaco	**Yes**	No	**Yes**	No
Montenegro	**Yes**	**Yes**	**Yes**	No
Russia	**Yes**	**Yes**	**Yes**	**Yes**

143. In some jurisdictions, the appointment of a Data Privacy Officer (DPO) may exempt the organization from its registration obligations.
144. This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

EUROPE/ EURASIA (NON-EEA) MANDATORY REQUIREMENTS				
COUNTRIES WITH PRIVACY LAWS	**REGIS-TRATION**	**DPO[143]**	**CROSS-BORDER LIMIT-ATIONS**	**DATA SECURITY BREACH NOTIFI-CATION[144]**
San Marino	**Yes**	No	**Yes**	No
Serbia[145]	**Yes**	No	**Yes**	No
Turkey	**Yes**	No	**Yes**	**Yes**
Ukraine	**Yes**	**Yes**	**Yes**	No

145. On November 21, 2018, a new Law on Personal Data Protection which mirrors the GDPR was adopted; the new Law will enter into force in July 2019.

NOTES

NOTES

6

An Overview of Cybersecurity Legal Requirements for All Businesses: 2019 Update

Thomas J. Smedinghoff

Locke Lord LLP

Thomas J. Smedinghoff is Of Counsel in the Privacy & Cybersecurity Practice Group at the law firm of Locke Lord LLP, in Chicago. He is Co-Chair of the ABA Cybersecurity Legal Task Force, and Chair of the Identity Management Legal Task Force and Co-Chair of the Cybersecurity Subcommittee of the ABA Section of Business Law, Cyberspace Committee. He is also a member of the U.S. Delegation to the United Nations Commission on International Trade Law ("UNCITRAL"), where he participated in the negotiation of the United Nations *Convention on the Use of Electronic Communications in International Contracts*. Mr. Smedinghoff is co-editor and contributing author of the GUIDE TO CYBERSECURITY DUE DILIGENCE IN M&A TRANSACTIONS (American Bar Association, 2017), and a contributing author to the 1st and 2nd editions of: THE ABA CYBERSECURITY HANDBOOK - A RESOURCE FOR ATTORNEYS, LAW FIRMS & BUSINESS PROFESSIONALS (ABA, 2013 and 2018). He is also the author of the book titled INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE, (2008). He can be reached at Tom.Smedinghoff@lockelord.com.

Table of Contents

A. WHAT IS DATA SECURITY? 7
B. THE DUTY TO PROVIDE SECURITY 9
1. Where Does the Duty to Provide Security Come From? 10
(a) Statutes and Regulations 10
(b) Common Law Obligations 14
(c) Rules of Evidence 15
(d) Contractual Obligations 16
(e) Self-Imposed Obligations 16
2. What Is the Nature of the Legal Obligation? 17
3. What Is the Legal Standard for Compliance? Defining "Reasonable" Security 18
(a) Identify Information Assets 22
(b) Conduct a Periodic Risk Assessment 22
(c) Select and Implement Responsive Security Controls to Manage and Control Risk 28
(1) Relevant Factors to Consider 29
(2) Categories of Security Measures that Must Be Addressed 30
(d) Monitoring and Testing 34
(e) Oversee Third Party Service Provider Arrangements 35
(f) Review and Adjustment 36
4. Special Rules for Specific Data Elements 37
(a) Sensitive Data 37
(b) Social Security Numbers 38
(c) Credit Card Data 38
5. Special Rules for Specific Security Controls 39
(a) Duty to Encrypt Data 39
(b) Data Destruction 39
6. A Safe Harbor for Reasonable Security? 40
C. THE DUTY TO WARN OF SECURITY BREACHES 43
1. The Basic Obligation 44
2. International Adoption 46
APPENDIX 47

What are the cybersecurity[2] legal obligations generally applicable to all U.S. businesses?

It is well known that certain sectors of the U.S. economy are subject to extensive regulations regarding data security. The most obvious examples are the financial sector,[3] the healthcare sector,[4] the federal government sector,[5] and other critical infrastructure sectors.[6] But what about companies in non-regulated sectors?

There is also no doubt that non-regulated businesses are subject to data security obligations. One need look no further than the numerous FTC and state attorney general enforcement actions since 2002 to see that regulated and non-regulated companies alike have been targeted for failure to provide appropriate data security for their own corporate data. Examples include software vendors (Microsoft[7] and Guidance Software[8]), consumer electronics companies (Genica and Computer Geeks),[9] mobile app developers (Delta Airlines),[10] clothing retailers (Guess![11] and Life Is Good[12]),

---

2. For purposes of this paper, the terms cybersecurity, data security, and information security are treated as synonymous.
3. Subject to the Gramm-Leach-Bliley Act ("GLB"), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC) (emphasis added).
4. Subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. 1320d-2 and 1320d-4, and HIPAA Security Regulations, 45 C.F.R. Part 164.
5. Subject to the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Sections 3541-3549.
6. See Presidential Executive Order, "Improving Critical Infrastructure Cybersecurity," February 12, 2013, at www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
7. FTC V. Microsoft (Consent Decree, Aug. 7, 2002), *available at* www.ftc.gov/os/caselist/0123240/0123240.shtm.
8. In the Matter of Guidance Software (Agreement Containing Consent Order, FTC File No. 062 3057, November 16, 2006), available at www.ftc.gov/opa/2006/11/guidance.htm.
9. In the Matter of Genica Corporation, and Compgeeks.com, FTC File No. 082-3113 (Agreement Containing Consent Order, February 5, 2009), available at www.ftc.gov/os/caselist/0823113.
10. See, "California Attorney General Sues Delta Air Lines for Failing to Have a Mobile App Privacy Policy," at http://bit.ly/W11J4T.
11. In the matter of Guess?, Inc. (Agreement containing Consent Order, FTC File No. 022 3260, June 18, 2003), *available at* www.ftc.gov/os/2003/06/guessagree.htm.
12. In the Matter of Life is good, Inc. (Agreement Containing Consent Order, FTC File No. 072 3046, January 17, 2008), available at www.ftc.gov/os/caselist/0723046.

music retailers (Tower Records),[13] animal supply retailers (PetCo),[14] general merchandise retail stores (BJs Wholesale,[15] TJX companies,[16] and Sears[17]), shoe stores (DSW),[18] restaurant and entertainment establishments (Dave & Busters[19] and Briar Group[20]), social media sites (Twitter[21] and Facebook[22]), bookstores (Barnes & Noble),[23] property management firms (Maloney Properties, Inc.),[24] and hotels (Wyndham).[25]

The thesis of this paper is that all businesses, whether regulated or not, are generally subject to legal duties regarding the security of their corporate data. Those duties can be summarized as: (1) a duty to protect the security of their corporate data, and (2) a duty to disclose security breaches when they occur. The following sections will explain the source

13. In the Matter of MTS, Inc., d/b/a Tower records/Books/Video (Agreement containing Consent Order, FTC File No. 032-3209, Apr. 21, 2004), *available at* www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf.
14. In the Matter of Petco Animal Supplies, Inc. (Agreement containing Consent Order, FTC File No. 042 3153, Nov. 7, 2004), *available at* www.ftc.gov/os/caselist/0323221/0323221.htm.
15. In the Matter of BJ's Wholesale Club, Inc. (Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005), *available at* www.ftc.gov/opa/2005/06/bjswholesale.htm.
16. In The Matter of The TJX Companies, Inc., FTC File No. 072-3055 (Agreement Containing Consent Order, March 27, 2008), available at www.ftc.gov/os/caselist/0723055.
17. In the Matter of Sears Holdings Management Corporation, FTC File No. 082 3099 (Agreement Containing Consent Order, September 9, 2009), available at http://www.ftc.gov/os/caselist/0823099/index.shtm.
18. In the Matter of DSW Inc., (Agreement containing Consent Order, FTC File No. 052 3096, Dec. 1, 2005), *available at* www.ftc.gov/opa/2005/12/dsw.htm.
19. In the Matter of Dave & Buster's, Inc., FTC File No. 082 3153 (Agreement Containing Consent Order, March 25, 2010), available at http://www.ftc.gov/os/caselist/0823153/index.shtm.
20. See "Massachusetts Attorney General Breaking New Ground in Data Security Enforcement?" at http://bit.ly/15rGiz4.
21. In the Matter of Twitter, Inc., FTC File No. 092 3093 (Agreement Containing Consent Order, June 24, 2010; Decision and Order, March 11, 2011), available at http://www.ftc.gov/os/caselist/0923093a/index.shtm.
22. In the Matter of Facebook, Inc., File No 092 3184 (Agreement Containing Consent Order, November 29, 2011), available at http://ftc.gov/os/caselist/0923184/index.shtm.
23. http://www.steptoe.com/assets/attachments/514.pdf.
24. See, "Massachusetts Attorney General Announces $15,000 Settlement with Property Management Firm" at http://bit.ly/GU8iNU.
25. FTC v. Wyndham Worldwide Corporation, 2015 U.S. App. LEXIS 14839; 2015-2 Trade Cas. (CCH) P79,269 (3rd Cir. Aug. 24, 2015); FTC v. Wyndham Worldwide Corp., 2014 U.S. Dist. LEXIS 47622 (D. N.J., April 7, 2014). Complaint and other information at http://www.ftc.gov/opa/2012/06/wyndham.shtm).

and scope of those duties. But first we begin with a general overview of the concept of data security itself.

A. WHAT IS DATA SECURITY?

Security is the protection of assets (such as buildings, equipment, cargo, inventory, and in some cases, people) from threats. Cybersecurity (or data security, or information security) has been generally described as "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities,"[26] and as "the process by which an organization protects and secures systems, media, and facilities that process and maintain information vital to its operations."[27]

The terms data security, information security and cybersecurity are often used interchangeably, although some might argue that each has a somewhat different emphasis. But regardless of the label, the focus is on the protection of both (1) *information systems*[28] – i.e., computer systems, networks, and software, and (2) the *data, messages, and information* that are typically recorded on, processed by, communicated via, stored in, shared by, transmitted, or received from such information systems.[29]

Measures designed to protect the security of information systems and data are generally grouped into three categories, which are typically referred to as follows:

---

26. ISO/IEC 27002:2005, *Information Technology – Security Techniques – Code of Practice for Information Security Management* (June. 2005), at p. viii (hereinafter "ISO 27002").
27. FFIEC, *IT Examinations Handbook – Information Security* (July 2006) at p. 1; available at http://ithandbook.ffiec.gov/it-booklets.aspx.
28. The Homeland Security Act of 2002 defines the term "information system" to mean "any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes – (A) computers and computer networks; (B) ancillary equipment; (C) software, firmware, and related procedures; (D) services, including support services; and (E) related resources." Homeland Security Act of 2002, Pub. L. 107-296, at Section 1001(b), amending 44 U.S.C. § 3532(b)(4).
29. The *data, messages, and information* to be protected potentially includes a wide variety of data, such as personally identifiable information about employees, customers, prospects, and other individuals; corporate financial information, information regarding corporate business transactions, trade secrets and other confidential information, information relating to corporate communications, including e-mail, and a variety of other types of corporate data. It can also take a variety of forms, including data, messages, documents, voice recordings, images, video, software, and other content in both electronic and paper form.

- **Physical security measures:** These are security measures which are designed to protect the tangible items that comprise the physical computer systems and networks that process, communicates, and store the data, including servers, devices used to access the system, storage devices, and the like. Examples include fences, walls, and other barriers; locks, safes, and vaults; armed guards; sensors and alarm bells.
- **Technical security measures:** These are security measures which involve the use of safeguards incorporated into computer hardware, software, and related devices. They are designed to ensure system availability, control access to systems and information, authenticate persons seeking access, protect the integrity of information communicated via and stored on the system, and ensure confidentiality where appropriate. Examples include: firewalls, intrusion detection software, access control software, antivirus software, passwords, PIN numbers, smart cards, biometric tokens, and encryption processes.
- **Administrative security measures:** Sometimes referred to as "procedural" or "organizational" security measures, these are security measures which consist of management procedures and constraints, operational procedures, accountability procedures, policies, and supplemental administrative controls to prevent unauthorized access and to provide an acceptable level of protection for computing resources and data. Administrative security procedures frequently include personnel management, employee use policies, training, and discipline.

Within each of these three categories, security measures are further classified as preventative, detective, or reactive. *Preventative* security measures are designed to prevent the occurrence of events that compromise security. An example of a preventative security measure is a lock on a door (to prevent access to a room containing computer equipment), or a firewall (to prevent unauthorized online access to a computer system). *Detective* security measures are designed to identify security breaches after they have occurred. An example of a detective security measure is a smoke alarm (which is designed to detect a fire), or intrusion detection software (which is designed to detect and track unauthorized online access to a computer system). *Reactive* security measures are designed to respond to a security breach, and typically include efforts to stop or contain the breach, identify the party or parties involved, and allow recovery of information that is lost or damaged. An example of reactive security is calling the police after an alarm detects that a burglary is in process, or shutting

down a computer system after intrusion detection software determines that an unauthorized user has obtained access to the system.

The *objectives* to be achieved through the use of security measures can be defined in terms of either the positive results to be achieved or the negative consequences to be avoided. The positive results to be achieved are typically described as (1) ensuring the *availability* of systems and information, (2) controlling *access* to systems and information, and (3) ensuring the *confidentiality, integrity, authenticity* of information [30] The harms to be avoided are often described as unauthorized access, use, disclosure or transfer, modification, alteration, or processing of data, and accidental loss or destruction of data.[31]

Achieving these objectives involves implementing security measures designed to protect systems and information from the various threats they face. What those threats are, where they come from, what is at risk, and how serious the consequences are, will of course, vary greatly from case to case. But responding to the threats a company faces with appropriate physical, technical, and organizational security measures is the focus of the duty to provide security.

B. THE DUTY TO PROVIDE SECURITY

Concerns regarding individual privacy, corporate governance, accountability for financial information, the authenticity and integrity of transaction data, and the confidentiality and security of sensitive business data are driving the enactment of new laws and regulations designed to ensure that businesses adequately address the security of their own data. In addition to sector-specific regulations, legislative and regulatory initiatives are imposing obligations on all businesses to implement information security

30. *See, e.g.*, GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.B; HIPAA Security Regulations, 45 C.F.R. Section 164.306(a)(1); REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "General Data Protection Regulation," or "**GDPR**"), at Article 31(b).
31. Many of the foreign privacy laws focus their security requirements from this perspective. This includes, for example, EU GDPR Article 32(2); Albania Act, Article 9; Argentina Act, Article 9(1); Australia Act, Schedule 3, Section 4.1; Canada Act, Schedule 1, Section 4.7.1; Hong Kong Act, Principle 4; Philippines Act, Article 8.1; Russia Act, Section 19(1); Singapore Model Code, Principle 7, Section 4.7.1; United Arab Emirates Act, Articles 15(1) and 16(1).

measures to protect their own data and to disclose breaches of security that do occur.

1. Where Does the Duty to Provide Security Come From?

There is no single law, statute, or regulation that governs a non-regulated company's obligations to provide security for its information. Corporate legal obligations to implement security measures are set forth in an ever-expanding patchwork of generally-applicable state, federal, and international laws, regulations, and enforcement actions, as well as common law duties and other express and implied obligations to provide "reasonable" or "appropriate" security for corporate data. And these obligations apply to both regulated and non-regulated industries.

When viewed as a group they cover a large segment of corporate activity. The most common sources of obligations to provide data security include the following:

(a) Statutes and Regulations

Numerous statutes and regulations impose obligations on businesses to provide security. Some are sector-specific comprehensive security regulations. Other generally-applicable laws are readily recognized by the fact that they are labeled as security laws or use terms such as "security," "safeguards," or "protection."[32] But in many cases the fact that they impose security obligations is evident only by their inclusion or use of terms relating to the attributes of security, such as "authenticate," "integrity," "confidentiality," "availability of data," and the like.[33] Some of the most common sources of statutory and regulatory obligations to provide cybersecurity include:

(1) **Privacy Laws.** The obligation to provide adequate security for personal data collected, used, and/or maintained by a business is a critical component of almost all privacy laws. Most statements of basic privacy principles include security as a key

32. See, e.g., Standards for the Protection of Personal Information of Residents of the Commonwealth, Massachusetts 201 CMR 17; and Business Duty to Protect Sensitive Personal Information, Tex. Bus. & Com. Code § 521.052.
33. *See, e.g.,* E-SIGN, 15 USC 7001 et seq. and UETA.

component,[34] and most privacy laws and regulations typically require companies to implement information security measures to protect certain personal data they maintain about individuals.

In the United States protecting personal information is the focus of numerous federal and state privacy laws and regulations. In addition to sector-specific privacy laws and regulations such as GLB (financial sector), HIPAA (healthcare sector), and the Privacy Act of 1974 (federal government), and numerous federal and state privacy laws that target specific types of data, also include security requirements. This includes the federal Children's Online Privacy Protection Act (COPPA), which applies to all businesses collecting personal information on the Internet from children, as well as numerous state laws relating to credit card information, personal information, and social security numbers.[35]

(2) **Data Security Laws and Regulations.** Separate from privacy laws, several states have enacted laws imposing a general obligation on all companies to ensure the security of personal information and other corporate data. The first was California, which enacted legislation in 2004 requiring all businesses to "implement and maintain reasonable security procedures and practices" to protect personal information about California residents from unauthorized access, destruction, use, modification, or disclosure.[36] Several other states have followed suit.[37] These include, most notably, the comprehensive Massachusetts data

---

34. *See, e.g.*, Consumer Privacy Bill of Rights in White House Report "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012; available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; Australia, Information Privacy Principles under the Privacy Act 1988, Principle No. 4, available at www.privacy.gov.au/publications/ipps.html; AICPA and the Canadian Institute of Chartered Accountants (CICA), Generally Accepted Privacy principles, Principle No. 8, available at http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles; APEC, Privacy principles, Principle No. 7, available at http://austlii.edu.au/~graham/APEC/APECv10.doc; US-EU Privacy Shield Privacy Principles, available at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg; Direct Marketing Association, Online Marketing Guidelines, available at www.the-dma.org/guidelines/onlineguidelines.shtml.
35. These include Arkansas, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah.
36. Cal. Civ. Code § 1798.81.5(b).
37. See list in Appendix.

security regulations,[38] and the New York State Department of Financial Services security regulations.[39] State laws governing secure data destruction also fall in to this category.

Some federal regulations also impose a duty to provide for the security of data and systems. Examples include IRS regulations that require companies to implement information security to protect electronic tax records, and SEC regulations regarding protection of corporate financial data,[40] as well as sector-specific regulations such as GLB and HIPAA.

(3) **E-Transaction Laws.** E-transaction laws require appropriate data security to ensure the enforceability of electronic records and for compliance with electronic recordkeeping requirements. Both the federal and state electronic transaction statutes (E-SIGN and UETA) require all companies to provide security for storage of electronic records relating to online transactions. For example, they focus on the security requirements of data integrity and accessibility, and require that an electronic record must "accurately reflect the information set forth in the record after it was first generated in its final form," and that it must "remain accessible for later reference."[41]

(4) **Corporate Governance Legislation.** Corporate governance legislation designed to protect the company and its shareholders, investors, and business partners, such as Sarbanes-Oxley and implementing regulations, require public companies to ensure that they have implemented appropriate information security controls with respect to their financial information.[42] In addition, SEC disclosure guidance issued on October 13,

38. 201 CMR 17.00 *et seq.*, available at http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf.
39. New York Department of Financial Services, Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500.02.
40. See, e.g., IRS Regulations: Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25, and SEC Regulations: 17 C.F.R. 240.17a-4, 17 C.F.R. 257.1(e)(3), and 17 C.F.R. § 248.30.
41. See e.g., UETA at Section 12. See also E-SIGN at 15 USC Sections 7001(d) and (e).
42. See generally, Bruce H. Nearon, Jon Stanley, Steven W. Teppler, and Joseph Burton, Life after Sarbanes-Oxley: The Merger of Information Security and Accountability, 45 Jurimetrics Journal 379-412 (2005).

2011[43] and updated on February 21, 2018,[44] identifies cyber risks and incidents as potential material information to be disclosed under existing securities law disclosure requirements and accounting standards.

(5) **Unfair & Deceptive Business Practice Laws.** Unfair business practice laws (such as FTC Act Section 5,[45] which prohibits "unfair or deceptive acts or practices in or affecting commerce," and equivalent state laws) and related government enforcement actions are frequently used as a basis for regulating security.

Through a series of enforcement actions and consent decrees beginning in 2002, both the FTC[46] and several state attorneys general have, in effect, extended security obligations regarding personal information to non-regulated industries by virtue of Section 5 of the FTC Act and similar state laws. Initially, cases were based on the alleged failure of companies to provide adequate information security contrary to representations they made to customers. In other words, these were claims of *deceptive trade practices*. But beginning in June 2005, the FTC significantly broadened the scope of its enforcement actions by asserting that a failure to provide appropriate information security for consumer personal information was itself, an *unfair trade practice* – even in the absence of any false representations by the defendant as to the state of its security.[47]

(6) **Breach Notification Laws.** In addition to the legal obligation to *implement* security measures to protect corporate data, many laws impose an obligation to *disclose* security breaches to the persons affected. But unlike laws that impose a duty to provide security, these laws typically require that companies disclose security breaches to those who may be adversely

43. SEC Guidance: SEC CF Disclosure Guidance: Topic No. 2, Cybersecurity; https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
44. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746, at https://www.sec.gov/rules/interp/2018/33-10459.pdf.
45. 15 USC Section 45.
46. See e.g., FTC security enforcement actions, listed a https://www.ftc.gov/enforcement/cases-proceedings/terms/249.
47. The FTC's authority to proceed in this manner was upheld in *FTC v. Wyndham Worldwide Corporation*, 2015 U.S. App. LEXIS 14839; 2015-2 Trade Cas. (CCH) P79,269 (3rd Cir. Aug. 24, 2015); affirming *FTC v. Wyndham Worldwide Corp.*, 2014 U.S. Dist. LEXIS 47622 (D. N.J., April 7, 2014).

affected by such breaches[48] and I man cases, to the state's attorney general.

All states in the U.S., plus the District of Columbia, Puerto Rico, and the Virgin Islands, have enacted security breach notification laws, all generally based on a 2003 California law.[49] The U.S. federal banking regulatory agencies also require financial institutions to disclose breaches,[50] and the HITECH Act and associated regulations also require notice in the event of a breach.[51] Internationally, many countries are also increasingly requiring breach notification.[52]

(b) Common Law Obligations

Some case law also recognizes that there may be a common law duty to provide data security, the breach of which constitutes a tort. Most recently, for example, in *Dittman v. UPMC* the Pennsylvania Supreme Court held that "in collecting and storing its employees' personal data on its computer systems, [the employer] owed its employees a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act."[53] Several years earlier, in *Bell v. Michigan Council*, a Michigan court held that "defendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information."[54] Likewise, in the case of *In re: Sony Gaming Networks and Customer Data Security Breach Litigation*, the court recognized the existence of a legal duty to provide security, noting as follows:

---

48. *Pisciotta v. Old National Bancorp*., 2007 U.S. App. Lexis 20068 (7th Cir. 23 August 2007), at p. 13.
49. See list of citations and links at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
50. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), March 29, 2005, Federal Register, Vol. 70, No. 59, 29 March 2005, at p. 15736 (hereinafter "Interagency Guidance").
51. 45 CFR Part 164.
52. See, e.g., the EU GDPR at Articles 33 and 34.
53. *Dittman v. UPMC*, No. J-20-2018, 2018 Pa. Lexis 6051(Pa. Nov 21, 2018), at pp. 16-17.
54. *Bell v. Michigan Council*, 205 Mich. App. Lexis 353 at *16 (Mich. App. 2005).

> Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law. See, e.g., Witriol v. LexisNexis Grp., No. C05-02392 MJJ, 2006 WL 4725713, at *8 (N.D. Cal. Feb. 10, 2006); CUMIS Ins. Soc'y., Inc. v. BJ's Wholesale Club, Inc., No. 051158, 2005 WL 6075375, at *4 (Mass. Super. Dec. 7, 2005) aff'd, 918 N.E.2d 36 (Mass. 2009); Yakubowicz v. Paramount Pictures Corp., 536 N.E.2d 1067, 1070 (Mass. 1989) ("A basic principle of negligence law is that ordinarily everyone has a duty to refrain from affirmative acts that unreasonably expose others to a risk of harm."). As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.55

(c) Rules of Evidence

Providing appropriate security necessary to ensure the integrity of electronic records (and, where necessary, the identity of the creator, sender, or signer of the record) will likely be critical to the admissibility of the electronic record in evidence in a future dispute. This conclusion is supported both by case law[56] as well as provisions relating to the form requirement for an "original" in electronic transaction legislation.[57]

In particular, the Ninth Circuit decision in the case of *American Express v. Vinhnee*[58] suggests that use of appropriate security may be a condition for the admissibility in evidence of electronic records. The bottom line is that, in many situations, the admissibility of all types of electronic data will depend, on the level of information security provided in order to ensure that the integrity and availability of the information remains intact.

---

55. *In re: Sony Gaming Networks and Customer Data Security Breach Litigation*, 2014 BL 15530, (S.D. Cal., No. 3:11-md-02258-AJB-MDD, partially dismissed Jan 21, 2014), at pp. 21-22.
56. *See, e.g.*, *American Express v. Vinhnee*, 2005 Bankr. Lexis 2602 (9th Cir. Bk. App. Panel, 2005); *Lorraine v. Markel*, 2007 U.S. Dist. Lexis 33020 (D. MD. May 4, 2007).
57. See, e.g., UETA Section 12, and E-SIGN, 15 USC Section 7001(d).
58. *American Express v. Vinhnee*, 336 B.R. 437; 2005 Bankr. Lexis 2602 (9th Cir. December 16, 2006).

(d) Contractual Obligations

Data security obligations are often imposed by contract as well. As businesses increasingly become aware of the need to protect the security of their own data, they frequently try to satisfy their obligation (at least in part) by contract in those situations where third parties will have possession of, or access to, their business data. This is particularly common, for example, in outsourcing and cloud service arrangements where a company's data will be stored with and/or processed by a third party. In addition, in any situation where a business may have access to data of a trading partner, it is quite common for the trading partner to contractually impose security obligations with respect to that data.

Security obligations are also typically imposed by contract in connection with participation in a multi-party system. For example, merchants desiring to accept credit cards must contractually agree to comply with the requirements of the Payment Card Industry Data Security Standard[59] as a condition of accepting credit cards. Similarly, businesses that want to originate electronic payment orders (e.g., to debit a customer's bank account) must agree to the rules of the applicable electronic payment systems (such as the ACH payment system), which rules include data security provisions.

(e) Self-Imposed Obligations

In many cases, security obligations are also self-imposed. This commonly occurs, for example, through statements in privacy policies, on websites, or in advertising materials, companies often make representations regarding the level of security they provide for their data (particularly the personal data they collect from the persons to whom the statements are made). See, *e.g., Equifax Ruling Shows How Cyber Boasts Can Bring Legal Pain*, Law360 (January 31, 2019).[60]

Likewise, when companies voluntarily self-certify under the U.S.-EU Privacy Shield Framework,[61] they represent that they comply with the seven Privacy Shield Principles.[62] Those Principles include a security requirement that "Organizations creating,

59. Available at www.pcisecuritystandards.org.
60. https://www.law360.com/banking/articles/1123080/equifax-ruling-shows-how-cyber-boasts-can-bring-legal-pain.
61. See generally https://www.privacyshield.gov.
62 . https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.

maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data."[63]

By making such public statements or representations, companies impose on themselves an obligation to comply with the standard they have represented to the public that they meet. If those statements are not true, or if they are misleading, such statements may become, in effect, deceptive trade practices under Section 5 of the FTC Act, or under equivalent state laws. Through a series of enforcement actions and consent decrees, both the FTC and several state attorneys general have used those deceptive business practice statutes to bring enforcement actions against the offending companies.

2. What Is the Nature of the Legal Obligation?

The duty to provide data security is often simply stated in the law as an obligation to implement "reasonable" or "appropriate" security measures designed to achieve the security objectives noted above.

In Europe, for example, the GDPR requires organizations to "implement *appropriate* technical and organisational measures to ensure a level of security appropriate to the risk."[64]

In the United States, state security laws, such as in California, generally require "*reasonable* security procedures and practices."[65] Federal laws and regulations do the same. For example, HIPAA requires "*reasonable and appropriate" security*,[66] and the GLB security regulations require security *appropriate* to the size and complexity of the bank and the nature and scope of its activities."[67]

In other words, the law views security as a relative concept, and recognizes that what qualifies as reasonable security varies with the situation. Thus, the law typically provides little or no guidance on what

63. Privacy Shield Principle No. 4.
64. GDPR Article 32(1) (emphasis added). See also UK – Data Protection Act 1998, Schedule 1, Part I, Seventh Principle.
65. Cal. Civil Code § 1798.81.5(b).
66. 42 U.S.C. 1320d-2(d)(2).
67. See, Gramm-Leach-Bliley Act ("GLB"), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC) (emphasis added).

specific security measures are required, or on how much security a business should implement to satisfy those legal obligations. Most laws do not include any specific requirements regarding whether or not a particular security measure must be implemented,[68] and there are generally no safe harbors.[69] In light of such standards, the choice of security measures and technology can vary depending on the situation.

3. What Is the Legal Standard for Compliance? Defining "Reasonable" Security

Laws requiring that companies implement "reasonable" or "appropriate" security often provide little or no guidance as to what is required for legal compliance. Legal developments over the past few years, however, suggest that a legal standard for "reasonable" security is clearly emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like), and instead adopts a fact-specific approach to corporate security obligations that requires a "process" applied to the unique facts of each case. It puts the focus on identifying and responding to the particular threats a business faces.

Rather than telling companies what specific security measures they must implement, the emerging legal standard requires companies to engage in an ongoing and repetitive process that is designed to identify and assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments. The decision regarding the specific security measures is left up to the company.

This approach recognizes that there are a variety of different security measures responsive to specific threats, and recognizes that threats (and appropriate responsive security measures) are constantly changing. Thus, the presence or absence of specific security measures says little about the status of a company's legal compliance with its information security obligations. Because armed guards at a the front of a building do not protect against hackers accessing information through the Internet, and because firewalls designed to stop hackers do not protect against dishonest employees with authorized access, the law puts its focus on

68. There are some exceptions, however. For example, the Massachusetts security regulations require implementation of firewalls, the use of virus software, and in certain cases, the use of encryption. See 201 CMR 17.

69. *But see* Ohio Data Protection Act, ORC 1354, discussed below.

implementing those security measures that respond to the specific threats a business faces.

At its essence implementing "reasonable" or "appropriate" security compliance requires a company to develop and implement a risk-based "security program" based on a process-oriented approach whereby it does the following:

- **Assign Responsibility:** Designate one or more employees to be responsible for the security program;
- **Identify Information Assets**: Identify the corporate information assets that need to be protected, including (1) data records containing personal information or other sensitive confidential information, and (2) information systems used to process, store, and communicate the relevant data, such as computing systems, networks, and storage media (including laptops and portable devices);
- **Conduct Risk Assessment:** Periodically conduct a risk assessment to identify and assess internal and external risks to the security, confidentiality, and/or integrity of its information assets, and evaluate the effectiveness of the safeguards currently in place for minimizing such risks;
- **Select and Implement Responsive Security Controls:** Select and implement appropriate physical, administrative, and technical security controls to minimize the risks identified in the risk assessment;
- **Monitor Effectiveness:** Regularly monitor and test the security controls that have been implemented to ensure that the security program is operating in a manner reasonably calculated to protect the information assets; and upgrade the security controls as necessary to limit risks;
- **Regularly Review Program:** Review and adjust the security program on a regular basis, including: (i) whenever there is a material change in business practices that could affect the security of the information, and (ii) following any incident involving a breach of security; and
- **Address Third Party Issues:** Take all reasonable steps to (1) verify that each third-party service provider that has access to the information assets has the capacity to protect such information assets in the manner required by the risk assessment; (2) obligate such party by contract to actually implement such security, and (3) take

reasonable steps to ensure that each third party service provider is actually applying such security measures as required by the contract.

A key aspect of this process is recognition that it is never completed. It is ongoing, and must be continually reviewed, revised, and updated.

This "risk-based" legal standard for corporate information security has come to be known as a requirement to develop, implement, and maintain a "comprehensive information security program" (WISP),[70] or simply a "security program."

The legal requirement for a such a risk-based security program was first set forth in a series of financial industry security regulations required under the Gramm-Leach-Bliley Act (GLBA) titled *Guidelines Establishing Standards for Safeguarding Consumer Information.* They were issued by the Federal Reserve, the OCC, FDIC, and the Office of Thrift Supervision, on February 1, 2001,[71] and later adopted by the FTC in its GLBA *Safeguards Rule* on May 23, 2002.[72] The same approach was also incorporated in the Federal Information Security Management Act of 2002 ("FISMA"),[73] and in the HIPAA *Security Standards* issued by the Department of Health and Human Services on February 20, 2003.[74]

Shortly thereafter, the FTC also adopted the view that the risk-based process-oriented approach to information security outlined in these regulations sets forth a general "best practice" for legal compliance that should apply to all businesses in all industries.[75] Thus,

---

70. *See, e.g.,* Massachusetts Security Regulations, 201 CMR 17.03. *See also* Massachusetts Office of Consumer Affairs, "Small Business Guide: Formulating A Comprehensive Written Information Security Program," available at http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf. See also, Information Security and Security Breach Notification Guidance, published by the Illinois Attorney General's Office, at http://illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guideance.pdf.
71. 66 Fed. Reg. 8616, February 1, 2001; 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision).
72. 67 Fed. Reg. 36484, May 23, 2002; 16 C.F.R. Part 314.
73. 44 U.S.C. Section 3544(b).
74. 45 C.F.R. Parts 164.
75. See, Prepared Statement of the Federal Trade Commission on Identity Theft: Innovative Solutions For An Evolving Problem, Presented by Lydia Parnes, Director, Bureau of Consumer Protection, Before the Subcommittee On Terrorism, Technology and Homeland Security of the Senate Committee on the Judiciary, United States Senate**,** March 21, 2007 at p. 7 (noting that "the FTC Safeguards Rule promulgated under the GLB Act serves as a good model" for satisfying the obligation to maintain reasonable and appropriate security); available at www.ftc.gov/os/

the FTC has, in effect, implemented this process oriented requirement for a risk-based security program in all of its decisions and consent decrees relating to alleged failures to provide appropriate information security.[76] The National Association of Insurance Commissioners has also recommended the same approach in its Insurance Data Security Model Law.[77]

In 2010 this approach was formally adopted by Massachusetts in its data security regulations, which require businesses to develop a comprehensive written information security program, and set out detailed requirements for such a security program.[78] Likewise, the 2017 New York DFS Regulations adopt the same approach.[79] In the EU, a similar requirement is referenced in GDPR.[80]

The importance of a written security program is also being recognized in recent statutory updates. A change to the Massachusetts breach notification statute, for example, requires companies to notify the Attorney General in the event of a data breach, and as part of that notification, to indicate whether they maintain a written information security program.[81]

In sum, the law recognizes what security consultants have been saying for some time: "security is a process, not a product."[82] Legal compliance with security obligations involves a risk-based process applied to the facts of each case in order to achieve an objective (i.e., to identify and implement the security measures appropriate for that situation), rather than the implementation of standard specific security

---

testimony/P065409identitytheftsenate03212007.pdf. See also, Prepared Statement of the Federal Trade Commission before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, U.S. House of Representatives on "Protecting Our Nation's Cyberspace," April 21, 2004, at p. 5 (noting that "security is an ongoing process of using reasonable and appropriate measures in light of the circumstances"), available at www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf.

76. *See, e.g.,* FTC Decisions and Consent Decrees listed at https://www.ftc.gov/enforcement/cases-proceedings/terms/249.
77. *See, e.g.,* National Association of Insurance Commissioners, "Insurance Data Security Model Law" (2017), available at https://www.naic.org/store/free/MDL-668.pdf. 78. 201 CMR 17.00 et. seq.
78. 201 CMR 17.00 et. seq.
79. N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500.02 and 500.03.
80 . GDPR, Article 32.
81. Mass. Gen. Laws. Ch. 93H, Section 3(b) (effective April 11, 2019).
82. Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (John Wiley & Sons, 2000) at page XII.

measures in all cases. Thus, there will likely be no hard and fast rules. Instead, the legal obligation regarding security focuses on what is reasonable under the circumstances to achieve the desired security objectives.

Based on existing law and regulations, the required steps for developing a comprehensive information security program as the means of achieving reasonable security may be summarized as follows:

(a) Identify Information Assets

In order to protect something, you need to know what it is, where it is, how it is used, how valuable it is, and so forth. Thus, when addressing data security, the first step is to identify the information assets to be protected so as to define the scope of the effort.

This involves taking an inventory of the data and information that that organization creates, collects, receives, uses, processes, stores, and communicates to others. It also requires examining the systems, networks and processes by which such data is created, collected, received, used, processed, stored, and communicated.

Understanding where the data and systems are located is also important. This requires identifying where in the organization (e.g., which office and which department), the data and systems are located, and who controls them. It also requires identifying in which jurisdictions (country and state or province) they are collected, processed, and stored, as this will impact which laws must be complied with.

Moreover, it is also important to consider the organization's data that is in the possession and control of a third party, such as an outsource service provider or cloud provider, as the organization is responsible for the security of all of its data regardless of who has actual possession of it

(b) Conduct a Periodic Risk Assessment

Implementing a comprehensive security program to protect these information assets requires a thorough assessment of the potential risks to the organization's information systems and data.

A ***risk assessment*** is the process of identifying, estimating, and prioritizing information security risks to the business.[83]

83. *See, generally*, NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments (September 2012); NIST Cybersecurity Framework, at p. 5.

The purpose of a risk assessment is to inform decision makers and support the development and implementation of "appropriate" and "reasonable" security controls to respond to the risks identified.

Risk is a measure of the extent to which the business is threatened by a potential circumstance or event. It is typically a function of: (i) the likelihood of the occurrence of an adverse event or threat, and (ii) the adverse impacts that would result if such an adverse event or threat does materialize. Thus, assessing risk requires: (i) identifying relevant *threats* to the business; (ii) identifying *vulnerabilities* both internal and external to the business; (iii) assessing the *likelihood* that such threats will occur and exploit the vulnerabilities to cause harm, and (iv) evaluating the *impact* (i.e., harm) to the business that may result if the threat does occur and is able to exploit the vulnerabilities. The end result is a determination of risk.[84]

- A ***threat*** is anything that has the potential to cause harm to the information assets. Examples of threats include: (i) hostile cyber or physical attacks; (ii) human errors of omission or commission; (iii) structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and (iv) natural and man-made disasters, accidents, and failures beyond the control of the organization, such as a fire, flood, or tornado; or (v) technical and personal threats such as from malware, a computer virus, the actions of a hacker, or the negligent mistake of an employee.

- A ***vulnerability*** is a flaw or weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source—i.e., that can be accidentally triggered or intentionally exploited by the threat to endanger or cause harm to an information asset. It might be a hole in the roof, a system with easy to guess passwords, unencrypted data on a laptop computer, disgruntled employees, or employees that simply do not understand what steps they need to take to protect the security of company data.

  - Most information system vulnerabilities can be associated with security controls that either have not been applied

84. NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012), at p. 1.

(either intentionally or unintentionally), or have been applied, but retain some weakness;

- Some vulnerabilities can arise "over time as organizational missions/business functions evolve, environments of operation change, new technologies proliferate, and new threats emerge. In the context of such change, existing security controls may become inadequate and may need to be reassessed for effectiveness;"
- Vulnerabilities can also be found in organizational governance structures (e.g., the lack of effective risk management strategies and adequate risk framing, poor intra-agency communications, inconsistent decisions about relative priorities of missions/business functions, or misalignment of enterprise architecture to support mission/business activities);
- Vulnerabilities can also be found in external relationships (e.g., dependencies on particular energy sources, supply chains, information technologies, and telecommunications providers), mission/business processes (e.g., poorly defined processes or processes that are not risk-aware), and enterprise/information security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems).[85]

- The ***likelihood*** that a threat will exploit a vulnerability to cause harm creates a ***risk***. Stated differently, where a threat intersects with a vulnerability, risk is present. For example, if the threat is rain, and the vulnerability is a hole in the roof, risk is the likelihood that it will rain, causing water to enter the building through the hole in the roof, and doing damage to the building and/or its contents. Similarly, if the threat is a hacker, and the vulnerability is open Internet access to a server containing sensitive data, risk is the likelihood that a hacker will enter the system and view, copy, alter, or destroy the sensitive data.
- The level of ***impact*** from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized

85. NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012), at p. 9.

modification of information, unauthorized destruction of information, or loss of information or information system availability.

In other words, ***risk*** is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

Risk assessment, then, requires a process of identifying vulnerabilities and threats to the information assets used by the company, and assessing the potential impact/harm that would result if a threat materializes. This forms the basis on which the company determines what countermeasures (i.e., security controls), if any, it should implement to reduce risk to an acceptable level. Thus, a risk assessment requires:

- Conducting a threat assessment to identify all reasonably foreseeable internal and external threats to the information and system assets to be protected;[86]
- Conducting a vulnerability assessment to identify the company's vulnerabilities that could be exploited by threat sources;
- Assessing the likelihood that each of the threats will materialize, and if so, the probability that it will exploit one or more of the vulnerabilities to cause harm — i.e., identifying the likelihood that threat sources with the potential to exploit weaknesses or vulnerabilities in the system will actually do so;
- Evaluating the potential damage that will result in such case; and
- Assessing the sufficiency of the security controls in place to guard against the threat.[87]

---

86. *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(1); Mass. Regulations 201 CMR 17.03(2)(b); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02 (b)(1).
87. *See, e.g.*, FISMA, 44 U.S.C. Sections 3544(a)(2)(A) and 3544(b)(1); GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III.B(2); Mass. Regulations 201 CMR 17.03(2)(b); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.09; *see also* NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments* (September 2012) at p. 29.

This risk assessment process will be the baseline against which security controls can be selected, implemented, measured, and validated. The goal is to understand the risks the business faces, and determine what level of risk is acceptable, in order to identify appropriate and cost-effective safeguards to combat that risk.

Numerous security laws and regulations expressly require a risk assessment as part of a comprehensive security program. And laws and regulations that do not expressly include such a requirement typically do so impliedly.

In the U.S., a risk assessment is expressly required by a variety of security statutes and regulations, such as GLB[88] and HIPAA[89] at the federal level, and the Massachusetts[90] and New York[91] security regulations at the state level. And it is impliedly required by most other security statutes and regulations when they impose an obligation to provide "reasonable" security. Likewise, the consent decrees entered in all FTC enforcement actions have expressly extended the banking and healthcare sector-specific requirements for a risk assessment to all industries generally.[92]

In addition, several U.S. courts have held that a risk assessment plays a key role in determining whether a duty will be imposed and liability found. In *Wolfe v. MBNA America Bank*, for example, a federal court held that where injury resulting from negligent issuance of a credit card (to someone who applied using the plaintiff's identity) is foreseeable and preventable, "the defendant has a duty to verify the authenticity and accuracy of a credit account application."[93] In *Bell v. Michigan Council*, the court held that where a harm was foreseeable, and the potential severity of the risk was high, the defendant was liable for failure to provide appropriate security to address the potential harm.[94] On the other hand, in *Guin v. Brazos Education*, the court held that where a proper risk

88. GLB Security Regulations, 12 CFR Part 364, Appendix B (FDIC), III.B; 16 CFR §314.4 (FTC).
89. HIPAA Security Regulations, 45 CFR Section 164.308(a)(1)(ii)(A).
90. Mass. Regulations, 201 CMR 17.03(2)(b).
91. N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.09(a).
92. The FTC data security cases and enforcement actions are *available at* www.ftc.gov/datasecurity.
93. *Wolfe v. MBNA America Bank*, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007).
94. *Bell v. Michigan Council*, 2005 Mich. App. Lexis 353 (Mich. App. February 15, 2005).

assessment was done, but a particular harm was not reasonably foreseeable, the defendant would not be liable for failure to defend against it.[95]

In the EU and other countries, a risk assessment is frequently a required element of the obligation to provide appropriate data security. Many data protection laws expressly require a risk assessment, including the recently implemented EU-wide General Data Protection Regulation (GDPR).[96] Many other laws, however, impliedly require a risk assessment, typically by requiring that the company must provide a level of security "appropriate to the risk."

In most cases, however, the law does not generally specify how to do a risk assessment. In the U.S. the banking regulators have referred financial institutions seeking general information on risk assessments to:[97] (1) the "Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards,"[98] and (2) the "FFIEC IT Examination Handbook, Information Security Booklet."[99] General information on conducting a risk assessment is also available in the National Institute of Standards and Technology (NIST) special publication 800-30, Rev. 1 "Guide for Conducting Risk Assessments."[100] Massachusetts also provides guidance in its "Small Business Guide: Formulating a Comprehensive Written Information Security Program."[101]

---

95. *Guin v. Brazos Higher Education Service*, Civ. No. 05-668, 2006 U.S. Dist. Lexis 4846 at *13 (D. Minn. Feb. 7, 2006) (finding that where a proper risk assessment was done, the inability to foresee and deter a specific burglary of a laptop was not a breach of a duty of reasonable care).
96. *See* GDPR, at Recital 83 and Article 32.
97. FFIEC, *Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment*, August 8, 2006 at p. 5, *available at* www.ffiec.gov/pdf/authentication_faq.pdf.
98. *Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards*, December 14, 2005, *available at* www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/default.htm.
99. FFIEC, *IT Examination Handbook, Information Security Booklet*, July 2006, *available at* www.http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.
100. *See* National Institute of Standards and Technology, "Risk Management Guide for Information Technology Systems," NIST Special Publication No. 800-30, Rev. 1; available at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.
101. *See* Massachusetts Office of Consumer Affairs, "Small Business Guide: Formulating A Comprehensive Written Information Security Program," available at http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf. See also, Information Security and Security Breach Notification Guidance, published

(c) Select and Implement Responsive Security Controls to Manage and Control Risk

Key to providing reasonable security is implementing security measures that are responsive to the specific risks that a company faces. In other words, merely implementing seemingly strong security measures is not, by itself, sufficient for legal compliance. Thus, the next step in the process of developing a comprehensive information security program is to select and implement appropriate physical, technical, and administrative security controls to manage and control the risks the company faces, as identified in the risk assessment.[102]

The key to providing legally-compliant security is that the specific security controls selected and implemented must be responsive to the company's fact-specific risk assessment.[103] In other words, merely implementing seemingly strong security measures is not, by itself, sufficient for legal compliance. Those security controls must be responsive to the particular threats a business faces, and must address its vulnerabilities.

Posting armed guards around a building, for example, sounds impressive as a security measure, but if the primary threat the company faces is unauthorized remote access to its data via the Internet, that particular security measure is of little value. Likewise, firewalls and intrusion detection software are often effective ways to stop hackers and protect sensitive databases, but if a company's major vulnerability is careless (or malicious) employees who succumb to phishing attacks or inadvertently (or intentionally) disclose passwords or protected information, then even those sophisticated

---

by the Illinois Attorney General's Office, at http://illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guideance.pdf.

102. *See, e.g.*, U.S., GLB Security Regulations (OCC), 12 C.F.R. Part 30 Appendix B, Part II.A; HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(B); FISMA, 44 U.S.C. Section 3544(b); Mass. Regulations 201 CMR 17.03(1); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02(b); EU General Data Protection Regulation, at Recital 83 and Article 32.

103. *See, e.g.*, Mass. Regulations 201 CMR 17.03(2)(b); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02(b); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500. 02(b) and 500.03; EU General Data Protection Regulation, at Recital 83 and Article 32.

technical security measures, while important, will not adequately address the insider risk.

The role of the risk assessment in selecting security controls was also stressed by the U.S. banking regulators in their response to questions relating to its regulations for strong authentication. When asked whether a financial institution could forgo a risk assessment and move immediately to implement additional strong authentication controls, the regulators responded with an emphatic "no." As they pointed out, the security requirements for authentication are risk-based, and thus, a risk assessment that sufficiently evaluates the risks and identifies the reasons for choosing a particular control should be completed before implementing any particular controls.[104]

When selecting responsive security controls to implement, there are a number of *factors* that the organization should take into account, as well as *categories of security controls* identified in the applicable security laws (and any additional categories that are suggested by the risk assessment), that should be considered to reduce the company's risks and vulnerabilities to a reasonable and appropriate level.[105] T

(1) Relevant Factors to Consider

In determining what security measures should be implemented within a particular organization, existing precedent recognizes that there is no "one size fits all" approach. Which security measures are appropriate for a particular organization will vary, depending upon a variety of factors.

Traditional negligence law suggests that the relevant factors are (1) the probability of the identified harm occurring (i.e., the likelihood that a foreseeable threat will materialize), (2) the gravity of the resulting injury if the threat does materialize, and (3) the burden of implementing adequate precautions.[106] In other words, the standard of care to be exercised in any particular case depends upon the circumstances of that

104. See, FFIEC, "*Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment*," August 8, 2006 at p. 5, *available at* https://www.ffiec.gov/pdf/authentication_faq.pdf.

105. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(1)(ii)(B); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02(b); EU General Data Protection Regulation, at Recital 83 and Article 32.

106. *See, e.g., United States v. Carroll Towing,* 159 F.2d 169, 173 (2d Cir. 1947).

case and on the extent of foreseeable danger.[107] Security regulations take a similar approach, and indicate that the following factors are relevant in determining what security measures should be implemented in a given case:

The following factors are most often cited in security statutes and regulations as relevant to determining what security controls should be implemented to address identified risks in a given case:

- The company's size, complexity, and capabilities
- The nature and scope of the business activities
- The nature and sensitivity of the information to be protected
- The company's technical infrastructure, hardware, and software security capabilities
- The state of the art re technology and security
- The costs of the security measures[108]

Interestingly, cost was the one factor mentioned most often, and certainly implies recognition that companies are not required to do everything theoretically possible.

The bottom line is that the legal appropriateness of any particular security control is not determined in the abstract. Instead, it must be determined on the basis of a risk assessment specific to the company and its business, in light of the factors identified above.

(2) Categories of Security Measures that Must Be Addressed

Specifying a process still leaves many businesses wondering, "What specific security measures should I implement?"

---

107. *See, e.g.*, *DCR Inc. v. Peak Alarm Co.,* 663 P.2d 433, 435 (Utah 1983); *see also Glatt v. Feist,* 156 N.W.2d 819, 829 (N.D. 1968) (the amount or degree of diligence necessary to constitute ordinary care varies with facts and circumstances of each case).
108. *See, e.g.,* U.S., HIPAA Security Regulations, 45 C.F.R. Section 164.306(b)(2); GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.A and Part II.C (OCC); 16 CFR §314.3(a) (FTC); FISMA, 44 U.S.C. Sections 3544(a)(2) and 3544(b)(2)(B); Mass. Regulations 201 CMR 17.03(1); EU General Data Protection Regulation, at Recital 83 and Article 32.

In other words, in developing a security program, what security measures or safeguards should be included?

Generally, the law does not require companies to implement specific security measures or use a particular technology. As expressly stated in the HIPAA security regulations, for example, companies "may use any security measures" reasonably designed to achieve the objectives specified in the regulations.[109] This focus on flexibility means that, like the obligation to use "reasonable care" under tort law, determining compliance may ultimately become more difficult, as there are unlikely to be any safe-harbors for security.

Nonetheless, many security statutes and regulations require that companies consider certain *categories* of security measures, even if the way in which each category is addressed is not specified. At a high level, most security laws and regulations, for example, require that businesses implement appropriate physical, technical, and administrative (or organizational) security controls.[110] Within each of these three very broad categories of security controls, there are many subcategories to consider. NIST Special Publication 800-53 provides a catalog of security and privacy controls to protect organizational operations and assets.[111]

Some laws and regulations go a step further, and identify certain more granular categories of security controls that businesses should consider, in light of the results of their risk assessments and the other factors noted above, such as access

---

109. HIPAA Security Regulations, 45 CFR Section 164.306(b)(1). There are some exceptions, however. For example, the Massachusetts security regulations require implementation of firewalls, the use of virus software, and in certain cases, the use of encryption. See 201 CMR 17.00.

110. *See, e.g.,* GLB Security Regulations, 12 CFR Part 364, Appendix B, II.A (FDIC); and 16 CFR §314.3(a) (FTC); HIPAA Security regulations, 45 CFR Section 164.308 (Administrative safeguards); 45 CFR Section 164.310 (Physical safeguard), and 45 CFR Section 164.312 (Technical safeguards); Mass. Regulations, 201 CMR 17.03(1); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.03(j); EU General Data Protection Regulation, Articles 5(f) and 32(1).

111. NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (Updated August 2017), https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf. While this is written to "establish security controls for federal information systems and organizations," it also notes that "Private sector organizations are encouraged to consider using these guidelines, as appropriate.".

controls, training and education, or incident response planning.[112] For example, many laws require companies to implement access control measures to ensure that only authorized persons can access sensitive data. But the laws typically say nothing about which access controls should be used. At most, they will sometimes define objectives or criteria that must be achieved (such as restricting access on a need to know basis, or requiring that access be terminated when an employee leaves the company). Thus (in the example of access controls), companies are free to select any types of access controls that achieve those objectives and are reasonable for the business in light of the results of its risk assessment. But the key is to consider which security controls within a designated category are appropriate for the company in light of its particular risk assessment.

The general categories of security measures mentioned most often in the various laws, regulations, and security standards include the following:

- **Physical Facility and Device Security Controls** – Procedures to safeguard the facility, measures to protect against destruction, loss, or damage of information due to potential environmental hazards (such as fire and water damage or technological failures), procedures that govern the receipt and removal of hardware and electronic media

112. *Requirement for Access Controls* See, e.g., 12 CFR Part 364 (FDIC), Appendix B, III.C.1.a; Security Regulations, 12 CFR Part 364 (FDIC), Appendix B, III.C.2; HIPAA Security Regulations, 45 CFR 164.308(a)(4) (administrative access controls), 164.310(a) (physical access controls), 164.310(a) (technical access controls); Mass. Regulations 201 CMR 17.03(2)(g), 17.04(1)(d), 17.04(2); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500.03, 500.07;

Requirement for Training and Education: See, e.g., GLB Security Regulations, 12 CFR Part 364 (FDIC), Appendix B, III.C.2; HIPAA Security Regulations, 45 CFR 164.308(5)(i); Mass. Regulations, 201 CMR 17.04(8); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500.14; EU General Data Protection Regulation, Article 39(1).

Requirement for Incident Response Planning: See, e.g., GLB Security regulations (FTC), 12 CFR Part 364, Appendix B, III.C.1(g); Mass. Regulations, 201 CMR 17.03(2)(j); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. §§ 500.03(e), 500.03(n), and 500.16; EU General Data Protection Regulation, Article 32(1)(c).

into and out of a facility, and procedures that govern the use and security of physical workstations.

- **Physical Access Controls** – Access restrictions at buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.
- **Technical Access Controls** – Policies and procedures to ensure that authorized persons who need access to the system have appropriate access, and that those who should not have access are prevented from obtaining access, including procedures to determine access authorization, procedures for granting and controlling access, authentication procedures to verify that a person or entity seeking access is the one claimed, and procedures for terminating access.
- **Intrusion Detection Procedures** – Procedures to monitor log-in attempts and report discrepancies; system monitoring and intrusion detection systems and procedures to detect actual and attempted attacks on or intrusions into company information systems; and procedures for preventing, detecting, and reporting malicious software (e.g., virus software, Trojan horses, etc.);
- **Employee Procedures** – Job control procedures, segregation of duties, and background checks for employees with responsibility for or access to information to be protected, and controls to prevent employees from providing information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- **System Modification Procedures** – Procedures designed to ensure that system modifications are consistent with the company's security program;
- **Data Integrity, Confidentiality, and Storage** – Procedures to protect information from unauthorized access, alteration, disclosure, or destruction during storage or transmission, including storage of data in a format that cannot be meaningfully interpreted if opened as a flat, plain-text file, or in a location that is inaccessible to unauthorized persons and/or protected by a firewall;

- **Data Destruction and Hardware and Media Disposal** – Procedures regarding final disposition of information and/ or hardware on which it resides, and procedures for removal from media before re-use of the media;
- **Audit Controls** – Maintenance of records to document repairs and modifications to the physical components to the facility related to security (e.g., walls, doors, locks, etc); and hardware, software, and/or procedural audit control mechanisms that record and examine activity in the systems;
- **Contingency Plan** – Procedures designed to ensure the ability to continue operations in the event of an emergency, such as a data backup plan, disaster recovery plan, and emergency mode operation plan;
- **Incident Response Plan** – A plan for taking responsive actions in the event the company suspects or detects that a security breach has occurred, including ensuring that appropriate persons within the organization are promptly notified of security breaches, and that prompt action is taken both in terms of responding to the breach (e.g., to stop further information compromised and to work with law enforcement), and in terms of notifying appropriate persons who may be potentially injured by the breach.
- **Awareness, Training and Education** – Training and education for employees to ensure that they understand their roles and responsibilities with respect to security, including communication to employees of applicable security policies, procedures, standards, and guidelines, implementing a security awareness program, periodic security reminders, and developing and maintaining relevant employee training materials, such as user education concerning virus protection, password management, and how to report discrepancies.

(d) Monitoring and Testing

Merely implementing security measures is not sufficient. Companies must also ensure that the security measures have been properly put in place and are effective. This includes conducting an assessment

of the sufficiency of the security measures in place to control the identified risks,[113] and conducting regular testing or monitoring of the effectiveness of those measures.[114] Existing precedent also suggests that companies must monitor compliance with its security program.[115] To that end, a regular review of records of system activity, such as audit logs, access reports, and security incident tracking reports[116] is also important.

(e) Oversee Third Party Service Provider Arrangements

In today's business environment it is also important to recognize that companies often rely on third parties, such as outsource providers and cloud providers, to handle much of their data. When corporate data is in the possession and under the control of a third party, this presents special challenges for ensuring security.

A company's responsibility for the security of its data includes not only the data in its possession and control, but also its data residing with such third parties. Regardless of who performs the work, the legal obligation to provide the security itself remains with the company. As it is often said, "you can outsource the work, but not the responsibility." Accordingly, third party relationships should be subject to the same risk management, security, privacy, and other protection policies that would be expected if a business were conducting the activities directly.[117]

Thus, any comprehensive information security program must address the security of a company's data held by third parties. Laws and regulations imposing information security obligations on businesses often expressly address requirements with respect to the

---

113. *See, e.g.*, the FTC data security cases and enforcement actions *available at* www.ftc.gov/datasecurity.
114. *See, e.g.*, GLB Security Regulations, 12 C.F.R. Part 30, Appendix B, Part III(c)(3); Mass. Regulations 201 CMR 17.03(h); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.05; EU General Data Protection Regulation, at Article 32(1)(d); and the FTC data security cases and enforcement actions *available at* www.ftc.gov/datasecurity.
115. *See, e.g.*, the FTC data security cases and enforcement actions available at www.ftc.gov/datasecurity.
116. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(1)(ii)(D).
117. *See, e.g.,* Office of the Comptroller of the Currency, Administrator of National Banks, OCC Bulletin 2001-47 on Third Party Relationships, November 21, 2001 (*available at* www.OCC.treas.gov/ftp/bulletin/2001-47.doc).

use of third party outsource providers.[118] First and foremost, they make clear that regardless of who performs the work, the legal obligation to provide the security itself remains with the company. As it is often said, "you can outsource the work, but not the responsibility." Thus, third party relationships should be subject to the same risk management, security, privacy, and other protection policies that would be expected if a business were conducting the activities directly.[119]

Accordingly, security laws and regulations typically impose three basic requirements on businesses that outsource: (1) they must exercise due diligence in selecting service providers,[120] (2) they must contractually require outsource providers to implement appropriate security measures,[121] and (3) they must monitor the performance of the outsource providers.[122]

(f) Review and Adjustment

Perhaps most significantly, the legal standard for information security recognizes that security is a moving target. Businesses must constantly keep up with every changing threats, risks, vulnerabilities, and security measures available to respond to them. It is a never-ending process. As a consequence, businesses must conduct periodic internal reviews to evaluate and adjust the information security program in light of:

---

118. *See, e.g.*, U.S., GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(2); HIPAA Security Regulations, 45 C.F.R. Section 164.308(b)(1) and 164.314(a)(2); Mass. Regulations 201 CMR 17.03(f); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.11; EU General Data Protection Regulation, at Articles 28 and 32.
119. See, e.g., Massachusetts Security Regulations, 201 CMR 17.02(2)(f).
120. *See, e.g.,* GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(1); Mass. Regulations 201 CMR 17.03(2)(f)(1); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.11.
121. *See, e.g.,* GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(2); HIPAA Security Regulations, 45 C.F.R. Section 164.308(b)(1) and 164.314(a)(2); Mass. Regulations 201 CMR 17.03(2)(f)(2); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. COMP. CODES R. & REGS. tit. 23. § 500.11.
122. *See, e.g.,* GLB Security Regulations, 12 C.F.R. Part 30 Appendix B, Part II.D(3); N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.11.

- The results of the testing and monitoring
- Any material changes to the business or arrangements
- Any changes in technology
- Any changes in internal or external threats
- Any environmental or operational changes
- Any other circumstances that may have a material impact.

In addition to periodic internal reviews, best practices and the developing legal standard may require that businesses obtain a periodic review and assessment (audit) by qualified independent third-party professionals using procedures and standards generally accepted in the profession to certify that the security program meets or exceeds applicable requirements, and is operating with sufficient effectiveness to provide reasonable assurances that the security, confidentiality, and integrity of information is protected.It should then adjust the security program in light of the findings or recommendations that come from such reviews.

4. Special Rules for Specific Data Elements

In addition to laws imposing general security obligations with respect to personal information, developing law is also imposing new obligations to protect specific data elements or sub-categories of personal data. That is, laws, regulations, and standards are beginning to focus on specific data elements, and imposing specific obligations with respect to such data elements. Prime examples include Social Security numbers, credit card transaction data, and other sensitive data.

(a) Sensitive Data

In the EU, the GDPR requires special treatment for particularly sensitive personal information – defined as "special categories" of personal data. Those special categories are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[123] Processing such sensitive data,

123. GDPR, Article 9.

according to EU interpretation, requires that "special attention" be given to data security aspects to avoid risks of unauthorized disclosure. In particular, "*[a]ccess by unauthorized persons must be virtually impossible and prevented*." [124]

In the United States, a de facto category of sensitive information has been defined by the various state security breach notification laws. As discussed below, these laws require special action (i.e., disclosure) in the event of a breach of security with respect to a subcategory of personal data generally considered to be sensitive because of its potential role in facilitating identity theft.

(b) Social Security Numbers

The security of Social Security numbers has been the particular focus of numerous state laws enacted in recent years (see list in Appendix). The scope of these laws ranges from restrictions on the manner in which Social Security numbers can be used to requirements for security when communicating and/or storing such numbers. For example, several states have enacted laws that prohibit requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the number is encrypted.[125]

(c) Credit Card Data

For businesses that accept credit card transactions, the Payment Card Industry Data Security Standards ("PCI Standards")[126] impose significant security obligations with respect to credit card data captured as part of any credit card transaction. The PCI Standards, jointly created by the major credit card associations, require businesses that accept MasterCard, Visa, American Express, Discover, and Diner's Club cards to comply. At least three states have now incorporated at least part of the PCI Standards in their law.[127]

---

124. Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/07/EN, WP 131, February 15, 2007, at pp. 19-20; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf. (emphasis in original).
125. *See* list of state laws in GAO Report, Social Security Numbers: Federal and State Laws Restrict Use of SSN's, Yet Gaps Remain, September 15, 2005 at Appendix III; available at www.gao.gov/new.items/d051016t.pdf.
126. Available at www.pcisecuritystandards.org.
127. See list in Appendix.

5. Special Rules for Specific Security Controls

(a) Duty to Encrypt Data

Some laws and regulations impose obligations to use encryption in certain situations. Initially this included state laws that mandate encryption of Social Security numbers for communication over the Internet.[128] More recently, however, some state laws prohibit the electronic transmission of any personal information to a person outside of the secure system of the business (other than a facsimile) unless the information is encrypted.[129] Most notable are the Massachusetts Regulations, which require businesses to encrypt personal information if it is stored on "laptops or other portable devices," "will travel across public networks," or will "be transmitted wirelessly."[130]

(b) Data Destruction

Many laws and regulations impose security requirements with respect to the manner in which data is destroyed. These regulations typically do not require the destruction of data, but seek to regulate the manner of destruction when companies decide to do so.

At the Federal level, both the banking regulators and the SEC have adopted regulations regarding security requirements for the destruction of personal data. Similarly, at the State level, several states have now adopted similar requirements.[131]

Such statutes and regulations generally require companies to properly dispose of personal information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. With respect to information in paper form, this typically requires implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that the information cannot be read or reconstructed. With respect to electronic information, such regulations typically require implementing and monitoring compliance with policies and procedures that require the destruction or erasure of

128. Ariz. Rev. Stat. § 44-1373, Cal. Civ. Code § 1798.85, Conn. Gen. Stat. § 42-470, Md. Commercial Law Code Ann. § 14-3402(4).
129. NRS 597.970.
130. 201 CMR 17.04(3) and (5).
131. See list in Appendix.

electronic media containing consumer personal information so that the information cannot practicably be read or reconstructed.[132]

6. A Safe Harbor for Reasonable Security?

A first-of-its-kind data security law, the recently enacted Ohio Data Protection Act[133] may signal the beginning of a new trend in the legal approach to corporate cybersecurity obligations. At the same time, it may provide some assistance to businesses struggling to ensure that they have implemented legally required data security.

The Ohio Data Protection Act (effective November 1, 2018) introduces two very important concepts relevant to cybersecurity compliance:

- First, the Act implicitly recognizes that compliance with selected industry norms and best practices provide legally compliant "reasonable security;" and
- Second, for businesses that follow one of the approaches designated in the Act, the Act provides a safe harbor in the form of an affirmative defense to any tort action that is brought against the business alleging that its failure to implement reasonable information security controls resulted in a data breach concerning personal information.

To obtain the benefit of the affirmative defense, a business must "create, maintain, and comply with a written cybersecurity program" that satisfies three requirements:

- It must "contain administrative, technical, and physical safeguards . . . ***that reasonably conform to an industry recognized cybersecurity framework*** as described in [the Act]."[134]
- It must "be designed to do all of the following with respect to the [personal and/or restricted information]," as applicable:
  - (1) Protect the security and confidentiality of the information;
  - (2) Protect against any anticipated threats or hazards to the security or integrity of the information;

132. See, e.g., 16 CFR Section 682.3.
133. ORC 1354 et. Seq.; https://www.ohioattorneygeneral.gov/Business/CyberOhio/Data-Protection-Act.
134. ORC 1354.02(A) (emphasis added).

- (3) Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates,[135] and

- The "scale and scope" of the cybersecurity program must be appropriate based on all of the following factors:
  - The size and complexity of the covered entity;
  - The nature and scope of the activities of the covered entity;
  - The sensitivity of the information to be protected;
  - The cost and availability of tools to improve in formation security and reduce vulnerabilities;
  - The resources available to the covered entity.[136]

Businesses that meet these requirements are entitled to an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in the courts of Ohio and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information, or restricted information.[137]

The "industry-recognized cybersecurity frameworks" that qualify for the safe harbor under the Act (and to which an organization's cybersecurity program must "reasonably conform") are the following –

For all businesses:

- NIST Cybersecurity Framework[138]
- NIST Special Publication 800-171 ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations")[139]

135. ORC 1354.02(B).
136. ORC 1354.02(C).
137. ORC 1354.02(D).
138. NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (April 16, 2018); available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
139. NIST SP 800-171, Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (December 2016); available at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-171r1.pdf.

- NIST Special Publications 800-53 [140] ("Security and Privacy Controls for Information Systems and Organizations") and 800-53A ("Assessing Security and Privacy Controls in Federal Information Systems and Organization")[141]
- The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework[142]
- Center for Internet Security, Critical Security Controls for Effective Cyber Defense[143]
- International Organization for Standardization / International Electrotechnical Commission 27000 Family of Information Security Standards - information security management systems ISO-27000 family[144]

For regulated businesses:

- HIPAA security requirements
- GLB security requirements
- FISMA
- Health Information Technology for Economic and Clinical Health Act
- PCI standard

This approach appears to recognize that cybersecurity programs based on any of the foregoing provide "reasonable security," and that providing "reasonable security" is a defense in the case of a breach.

This Ohio statute is the first cybersecurity law providing an express safe harbor for entities that exercise "reasonable security". However, it should be noted that a few years ago the California Attorney

140. NIST SP 800-53, Rev 5, "Security and Privacy Controls for Information Systems and Organizations,(August 2017); available at https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf.
141. NIST SP 800-53A, Rev 4, Assessing Security and Privacy Controls in Federal Information Systems and Organization (December 18, 2014); available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.
142. FedRAMP Security Assessment Framework, Ver. 2.4 (November 15, 2017); available at https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf.
143. CIS Controls, available at https://www.cisecurity.org/controls/.
144. ISO/IEC 27000 Family of Information Security Standards, https://www.itgovernance.co.uk/iso27000-family.

General released a report setting forth what might be described as a reverse safe harbor – i.e., if you don't take certain steps, then you will be deemed *not* to have provided legally compliant reasonable security.

In the "California Data Breach Report 2012 – 2015,"[145] the California Attorney General referenced the requirement under California law that businesses implement "reasonable" security,[146] and noted that the Center for Internet Security's Critical Security Controls for Effective Cyber Defense (the Controls)[147] are designed to address this challenge.[148] But then the Report went further, stating that failure to implement those Controls constitutes a lack of reasonable security. Specifically, the Report states that:

> The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. *The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security*."[149]

It is unclear whether either the safe harbor approach adopted by the Ohio statute or the so-called reverse safe harbor approach promoted by the California Attorney General will gain traction. But as businesses struggle with the issue of defining "reasonable security," we can probably expect to see more law and regulation along these lines.

C. THE DUTY TO WARN OF SECURITY BREACHES

In addition to the duty to *implement* security measures to protect data, we are also witnessing a global trend to enact laws and regulations that impose

145. California Data Breach Report 2016, California Attorney General (February 2016), at p. 27-34. https://oag.ca.gov/breachreport2016.
146. See Cal. Civ. Code § 1798.81.5(b), "A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.".
147. The CIS Critical Security Controls for Effective Cyber Defense, Version 6, October 15, 2015, available from the Center for Internet Security at www.cisecurity.org/. Formerly known as the SANS Top 20, the Controls are now managed by the Center for Internet Security (CIS), a non-profit organization that promotes cybersecurity readiness and response by identifying, developing, and validating best practices.
148. Id, at p. 30.
149. Id. (emphasis added).

an obligation to *disclose* security breaches to the persons affected, and in many case to regulators as well.

Designed as a way to help protect persons who might be adversely affected by a security breach of their personal information, these laws impose on companies an obligation similar to the common law "duty to warn" of dangers. Such a duty is often based on the view that a party who has a superior knowledge of a danger of injury or damage to another that is posed by a specific hazard must warn those who lack such knowledge. By requiring notice to persons who may be adversely affected by a security breach (e.g., persons whose compromised personal information may be used to facilitate identity theft), these laws seek to provide such persons with a warning that their personal information has been compromised, and an opportunity to take steps to protect themselves against the consequences of identity theft.[150]

All states in the U.S. have now enacted security breach notification laws, all generally based on a 2003 California law.[151] These laws are generally applicable to all businesses that maintain data about residents of the enacting state.

1. The Basic Obligation

Taken as a group, the state and federal security breach notification laws generally require that any business in possession of sensitive personal information about a covered individual must disclose any breach of such information to the person affected. The key requirements, which vary from state-to-state, include the following:

- **Type of information** – The statutes generally apply to unencrypted sensitive personally identified information – e.g., information consisting of first name or initial and last name, plus one of the following: social security number, drivers license or other state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required for access to the account). In some states this list is longer, and may also include medical information, insurance policy numbers, passwords by themselves, biometric information, professional

150. *See, e.g.*, Recommended Practices on Notice of Security Breach Involving Personal Information, Office of Privacy Protection, California Department of Consumer Affairs, April, 2006 (hereinafter "California Recommended Practices"), at pp. 5-6 (available at www.privacy.ca.gov/recommendations/secbreach.pdf); Interagency Guidance *supra* note 4 , at p. 15752.
151. See list of statutes in Appendix.

license or permit numbers, telecommunication access codes, mother's maiden name, employer ID number, electronic signatures, and descriptions of an individual's personal characteristics.

- **Definition of breach** – Generally the statutes require notice following the unauthorized acces to or acquisition of computerized data that compromises the security, confidentiality or integrity of such personal information. In some states, however, notice is not required unless there is a reasonable basis to believe that the breach will result in substantial harm or inconvenience to the customer.
- **Who must be notified** – Notice must be given to any residents of the state whose unencrypted personal information was the subject of the breach. If a business maintains computerized personal information that the business does not own or license, the business must notify the owner of the information, rather than the individuals themselves. In addition, many states also require notice to the state Attorney General or other relevant regulator.
- **When notice must be provided** – Generally, persons must be notified in the most expedient time possible and without unreasonable delay, although some states now impose a specific time limits, such as 30 days after learning of the breach. In manyt states the time for notice may be extended for the following reasons:
  - ✓ Legitimate needs of law enforcement, if notification would impede a criminal investigation
  - ✓ Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system
- **Form of notice** – Notice may be provided in writing (e.g., on paper and sent by mail), in electronic form (e.g., by e-mail, but only provided the provisions of E-SIGN[152] are complied with), or by substitute notice.
- **Substitute notice options** – If the cost of providing individual notice is greater than a certain amount (e.g., $250,000) or if more than a certain number of people would have to be notified (e.g., 500,000), substitute notice may be used, consisting of:
  - ✓ E-mail when the e-mail address is available, and

152. 15 USC Section 7001 *et. seq*. This generally requires that companies comply with the requisite consumer consent provisions of E-SIGN at 15 USC Section 7001(c).

- ✓ Conspicuous posting on the company's web site, and
- ✓ Publishing notice in all major statewide media.

Several of these issues vary from state to state, however, and some have become controversial. One key issue revolves around the nature of the triggering event. In some states, for example, notification is required whenever there has been an unauthorized access that compromises the security, confidentiality, or integrity of electronic personal data. In other states, however, unauthorized access does not trigger the notification requirement unless there is a reasonable likelihood of harm to the individuals whose personal information is involved[153] or unless the breach is material.[154]

2. International Adoption

Although the breach notification concept began in the United States, it is rapidly spreading internationally. The EU formalized breach notification requirements via GDPR in 2018,[155] as did Canada.[156] Several other countries also impose some sort of duty to notify of security breaches including Chile, India, Mexico, Qatar, Russia, and South Korea.

153. Arkansas, Connecticut, Delaware, and Louisiana are examples of states in this category.
154. Montana and Nevada are examples of states in this category.
155. GDPR Articles 33 and 34.
156. Breach of Security Safeguards Regulations: SOR/2018-64, at http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html.

APPENDIX

Key Information Security Law References

A. Federal Statutes

1. **COPPA**: Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 *et seq*.
2. **CFPB**: Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. §§5531(a), 5536(a)(1)
3. **E-SIGN**: Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001(d).
4. **FCRA/FACTA:** Fair Credit Reporting Act,
5. **FISMA**: Federal Information Security Management Act of 2002, 44 U.S.C. Sections 3541-3549.
6. **FTC Act:** Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), prohibits unfair or deceptive acts or practices in or affecting commerce.
7. **GLB Act**: Gramm-Leach-Bliley Act, Public L. 106-102, Sections 501 and 505(b), 15 U.S.C. Sections 6801, 6805.
8. **HIPAA**: Health Insurance Portability and Accountability Act, 42 U.S.C. 1320d-2 and 1320d-4. See also Subtitle D of Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), at sections 13401 *et. seq*.
9. **Homeland Security Act of 2002**: 44 U.S.C. Section 3532(b)(1).
10. **Privacy Act of 1974:** 5 U.S.C. Section 552a
11. **Sarbanes-Oxley Act**: Pub. L. 107-204, Sections 302 and 404, 15 U.S.C. Sections 7241 and 7262.
12. **Federal Rules of Evidence 901(a):** *see American Express v. Vinhnee*, 2005 Bankr. LEXIS 2602 (9th Cir. Bk. App. Panel, 2005), and *Lorraine v. Markel*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007).

B. State Statutes

1. **UETA**: Uniform Electronic Transaction Act, Section 12 (now enacted in 47 states).

2. **Law Imposing Obligations to Provide Security for Personal Information**:

Arkansas	Ark. Code Ann. § 4-110-104(b)
California	Cal. Civ. Code § 1798.81.5
Connecticut	Conn. Gen. Stat. § 42-471
Delaware	Del Code, Title 6, § 12B-100
Florida	Fla. Stat. § 501.171(2)
Illinois	815 ILCS 530/45; (also 740 ILCS 14/1 re Biometric Information Privacy Act)
Louisiana	La. R.S. 51: 3074
Maryland	Md. Com. Law Code Ann. § 14-3503
Massachusetts	Mass. Gen. Laws. Ch. 93H, § 2(a); Regulations at 201 CMR 17.00 et. seq
Nevada	Nev. Rev. Stat. 603A.210
New Jersey	N.J.A.C. 13:45F-3 (Pre-Proposed New Rules – 12/15/08)
Oregon	Or. Rev. Stat. Section 646A.622
Rhode Island	R.I. Stat. 11-49.2-2(2) and (3)
Texas	Tex. Bus. & Com. Code Ann. § 521.052
Utah	Utah Code Ann. § 13-44-201

3. **Law Imposing Obligations to Provide Security for Medical Information**:

California	Confidentiality of Medical Information Act (CMIA) (Civ. Code, § 56 et seq.)

4. **Law Imposing Obligations to Provide Security for Credit Card Information**:

Minnesota	Minn. Stat. Chapter 325E.64
Nevada	Nev. Rev. Stat. 603A.215
Washington	RCWA Chapter 19.255

5. **Law Imposing Duty to Encrypt Personal Information**:

Arizona	Ariz. Rev. Stat. § 44-1373
California	Cal. Civil Code Section 1798.85(a)(3) [SSN]
Connecticut	Conn. Gen. Stat. § 42-470
Maryland	Md. Comm. Code § 14-3302(a)(3) [SSN]
Massachusetts	Mass. Gen. Laws. Ch. 93H, § 2(a); Regulations at 201 CMR 17.00 et. seq. [Personal Information on laptops, etc]
Nevada	Nev. Rev. Stat. 603A.215

6. **Data Disposal / Destruction Laws**:

Alaska	Ala. Stat. §§ 45.48.500 – 45.48.590
Arkansas	Ark. Code Ann. § 4-110-104(a)
California	Cal. Civil Code § 1798.81.
Connecticut	Conn. Gen. Stat. § 42-471
Delaware	H.B. 295 (2014), Del. Code §50C-101 et. seq.
Florida	Fla. Stat. § 501.171(8)
Georgia	Ga. Stat § 10-15-2
Hawaii	Haw. Stat Section § 487R-2
Illinois	815 ILCS 530/40 (all); 815 ILCS 530/30 (state agencies)
Indiana	Ind. Code § 24-4-14
Kentucky	Ken. Rev. Stat. § 365.720
Maryland	Md. Code, § 14-3502; Md. HB 208 & SB 194
Massachusetts	Mass. Gen. laws. Ch. 93I
Michigan	MCL § 445.72a
Montana	Mont. Stat. § 30-14-1703
Nevada	Nev. Rev. Stat. 603A.200
New Jersey	N.J. Stat. 56:8-162
North Carolina	N.C. Gen. Stat § 75-64
Oregon	2007 S.B. 583, Section 12
Texas	Tex. Bus. & Com. Code Ann. § 48.102(b)
Utah	Utah Code Ann. § 13-42-201

Vermont	Vt. Stat. Tit. 9 § 2445 et seq.
Washington	RCWA 19.215.020

7. **Security Breach Notification Laws**

Alabama	2018 S.B. 318, Act No. 396
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 18-545
Arkansas	Ark. Code §§ 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. §§ 36a-701b, 4e-70
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 *et seq.*
Idaho	Idaho Stat. §§ 28-51-104 to -107
Illinois	815 ILCS §§ 530/1 to 530/25
Indiana	Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 et seq.
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. §§ 51:3071 *et seq*.
Maine	Me. Rev. Stat. tit. 10 § 1346 *et seq.*
Maryland	Md. Code Com. Law §§ 14-3501 *et seq.,* Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass. Gen. Laws § 93H-1 *et seq.*
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500

Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801 *et seq.*
Nevada	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21
New Jersey	N.J. Stat. § 56:8-161 *et seq.*
New Mexico	2017 H.B. 15, Chap. 36 (effective 6/16/2017)
New York	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208
North Carolina	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208
North Dakota	N.D. Cent. Code §§ 51-30-01 *et seq.*
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166
Oregon	Oregon Rev. Stat. §§ 646A.600 to .628
Pennsylvania	73 Pa. Stat. §§ 2301 *et seq.*
Rhode Island	R.I. Gen. Laws §§ 11-49.3-1 *et seq.*
South Carolina	S.C. Code § 39-1-90
South Dakota	S.D. Cod. Laws §§ 20-40-20 to -46 (2018 S.B. 62)
Tennessee	Tenn. Code §§ 47-18-2107; 8-4-119
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053
Utah	Utah Code §§ 13-44-101 *et seq.*
Vermont	Vt. Stat. tit. 9 §§ 2430, 2435
Virginia	Va. Code §§ 18.2-186.6, 32.1-127.1:05
Washington	Wash. Rev. Code §§ 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98

Wyoming	Wyo. Stat. §§ 40-12-501 *et seq*
District of Columbia	D.C. Code §§ 28- 3851 *et seq.*
Guam	9 GCA §§ 48-10 et seq.
Puerto Rico	10 Laws of Puerto Rico §§ 4051 *et seq*
Virgin Islands	V.I. Code tit. 14, §§ 2208, 2209 502

8. **State SSN Laws**

Alaska	Ala. Stat. §§ 45.48.400 – 45.48.480
Arizona	Ariz. Rev. Stat. § 44-1373
Arkansas	Ark. Code Ann. § 4-86-107; § 6-18-208
California	Cal. Civ. Code § 1798.85; Cal. Fam. Code § 2024.5
Colorado	Colo. Rev. Stat. § 6-1-715; Colo. Rev. Stat. §13-21-109.5; Colo. Rev. Stat. § 23-5-127; Colo. Rev. Stat. § 24-72.3-102;
Connecticut	Conn. Gen. Stat. § 42-470; Conn. Gen. Stat. § 8-64b
Delaware	Del. Code Ann., tit. 7 § 503
Florida	Fla. Stat. ch. 97.0585
Georgia	Ga. Code Ann. § 50-18-72; O.C.G.A. § 10-1-393.8
Guam	5 GCA § 32704; 5 GCA § 32705
Hawaii	Haw. Rev. Stat. § 12-32; Haw. Rev. Stat. § 487J-2; Haw. Rev. Stat. § 12-3
Illinois	815 Ill. Comp. Stat. 505/2QQ; § 815 ILCS 505/2RR
Indiana	Ind. Code § 4-1-10-1 et seq.; Ind. Code § 9-24-6-2; Ind. Code § 9-24-9-2; Ind. Code § 9-24-11-5; Ind. Code § 9-24-16-3; Ind. Code § 4-1-8-5
Kansas	K.S.A. § 75-3520

Louisiana	La. Rev. Stat. Ann. § 17:440; La. Rev. Stat. Ann. § 18:154; La. Rev. Stat. Ann. § 32:409.1; La. Rev. Stat. Ann. § 37:23; La. Rev. Stat. Ann. § 44:11 ; La. Civ. Code § 3352
Maine	10 M.R.S. § 1272-B
Maryland	Md. Code Ann., Com. Law § 14-3402.
Massachusetts	Mass. Gen. Laws Ch. 167B, § 14 & § 22
Michigan	Mich. Comp. Laws § 445.81 et seq..
Minnesota	Minn. Stat. § 325E.59
Mississippi	Miss. Code Ann. § 25-1-111
Missouri	Mo. Rev. Stat. § 407.1355
Montana	Mont. Code Ann. § 32-6-306; Mont. Code § 30-14-1702, § 30-14-1703
Nebraska	Neb. Rev. Stat. § 48-237
Nevada	Nev. Rev. Stat. Chapter 239; Nev. Rev. Stat. Chapter 239B.030; Chapter 239B; Chapter 603
New Jersey	N.J. Stat. Ann. § 47:1-16; N.J. Stat. Ann. § C.56:8-164
New Mexico	N.M. Stat. Ann. § 57-12B-1 et seq.
New York	N.Y. Gen. Bus. Law § 399-dd
North Carolina	N.C. Gen. Stat. § 75-62
North Dakota	N.D. Cent. Code § 39-06-14
Oklahoma	Okla. Stat. tit. 40, § 173.1
Oregon	Or. Rev. Stat. § 107.840
Pennsylvania	74 Pa. Stat. Ann. §§ 201 to 204
Rhode Island	R.I. Gen. Laws § 6-13-17 and § 6-13-19
South Carolina	S.C. Code Ann. § 7-5-170; S.C. Code § 37-20-180
South Dakota	S.D. Codified Laws § 32-12-17.10; S.D. Codified Laws § 32-12-17.13
Texas	Tex. Bus. & Com. Code Ann. 35.48; Tex. Bus. & Com. Code Ann. 35.58; Tex. Elec Code Ann. § 13.004; Tex. Bus. & Com. Code § 20.02

Utah	Utah Code Ann. § 31A-21-110
Vermont	9 V.S.A. § 2440; 2030
Virginia	Va. Code Ann. § 2.2-3808; Va. Code Ann. § 59.1-443.
Washington	Rev. Code Wash. (ARCW) § 19.146.205
West Virginia	W. Va. Code § 17E-1-11
Wisconsin	Wis. Stat. § 36.32

9. **State SSN Laws Requiring SSN Policies**

Connecticut	H.B 5658
Michigan	Mich. Comp. Laws Section 445.84
New Mexico	N.M. Stat. Sections 57-12B-2-57-12B-3
New York	NY Gen. Bus. Law Section 3990dd(4)
Texas	Texas Bus. & Com. Code Sections 35.581 (effective through March 31, 2009)

C. Federal Regulations

1. **Regulations Imposing Obligation to Provide Security**

   (a) **COPPA Regulations**: 16 C.F.R. 312.8.

   (b) **DHS Regulations:** Electronic Signature and Storage of Form I-9, Employment Eligibility Verification, 8 C.F.R. Part 274a(2) (e), (f), (g), and (h) (requiring an effective records security program).

   (c) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at Paragraphs 33-36; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf.

   (d) **FDA Regulations:** 21 C.F.R. Part 11.

   (e) **FFIEC Guidance:** Authentication in an Internet Banking Environment , October 12, 2005, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. See also "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment," August 8,

2006 at p. 5, available at http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf; and Supplement to Authentication in an Internet Banking Environment, available at http://www.fdic.gov/news/news/press/2011/pr11111a.pdf.

(f) **GLB Security Regulations**: Interagency Guidelines Establishing Standards for Safeguarding Consumer Information (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 570 (Office of Thrift Supervision), and 16 C.F.R. Part 314 (FTC).

(g) **GLB Security Regulations (FTC)**: FTC Safeguards Rule (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 16 C.F.R. Part 314 (FTC).

(h) **HIPAA Security Regulations**: Final HIPAA Security Regulations, 45 C.F.R. Part 164.

(i) **HIPAA Breach Notification Rules**: 45 CFR Sections 164.400 – 164.414.

(j) **IRS Regulations**: Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.

(k) **IRS Regulations**: IRS Announcement 98-27, 1998-15 I.R.B. 30, and Tax Regs. 26 C.F.R. § 1.1441-1(e)(4)(iv).

(l) **SEC Guidance:** SEC CF Disclosure Guidance: Topic No. 2, Cybersecurity; http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

(m) **SEC Regulation S-P:** 17 C.F.R. § 248.

(n) **SEC Regulations**: 17 C.F.R. 240.17a-4, and 17 C.F.R. 257.1(e)(3).

(o) **SEC Regulations**: 17 C.F.R. § 248.30 Procedures to safeguard customer records and information; disposal of consumer report information (applies to any broker, dealer, and investment company, and every investment adviser registered with the SEC).

2. **Regulations Imposing Authentication Requirements**

(a) **ACH Operating Rules** (2005) Section 2.10.2.2 ("Verification of Receiver's Identity")

(b) **Banking Know Your Customer Rules**

i. 31 CFR § 103.121, Customer Identification Programs for banks, savings associations, credit unions, and certain non-Federally regulated banks

ii. 31 CFR § 103.122, Customer identification programs for broker-dealers

iii. 31 CFR § 103.123, Customer identification programs for futures commission merchants and introducing brokers

iv. 31 CFR § 103.131, Customer identification programs for mutual funds

(c) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at Paragraphs 13-25; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

(d) **FFIEC Guidance**: Authentication in an Internet Banking Environment , October 12, 2005, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. See also and Supplement to Authentication in an Internet Banking Environment, available at http://www.fdic.gov/news/news/press/2011/pr11111a.pdf.

(e) **USA PATRIOT Act**

i. 31 U.S.C. 5318 – Section 326 – "Verification of Identification"

ii. Know your customer rules

(f) **UN Convention on the Use of Electronic Communications in International Contracts** – Article 9

3. **Data Disposal / Destruction Regulations**

(a) **FCRA Data Disposal Rules**: 12 C.F.R. Parts 334, 364

(b) **SEC Regulations**: 17 C.F.R. § 248.30 Procedures to safeguard customer records and information; disposal of consumer report information (applies to any broker, dealer, and investment

company, and every investment adviser registered with the SEC).

4. **Security Breach Notification Regulations**

   (a) **FCC Order re Pretexting**, April 2, 2007 – In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, April 2, 2007, at paragraphs 26-32; available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf

   (b) **GLB Security Breach Notification Rule**: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), available at http://ithandbook.ffiec.gov/media/resources/3488/ots-ceo-ltr-214.pdf.

   (c) **IRS Regulations**: Rev. Proc. 97-22, 1997-1 C.B. 652, 1997-13 I.R.B. 9, and Rev. Proc. 98-25.

   (d) **HIPAA Amendments:** Subtitle D of Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), at sections 13401 *et. seq*

   (e) **SEC Guidance:** SEC CF Disclosure Guidance: Topic No. 2, Cybersecurity; http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

D. State Regulations

1. **Insurance – NAIC Model Regulations**: National Association of Insurance Commissioners, Standards for Safeguarding Consumer Information, Model Regulation.

2. **Attorneys** – New Jersey Advisory Committee on Professional Ethics, Opinion 701 (2006) available at http://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf

E. Best Practices Guidelines Issued by Government Agencies

1. California – California Attorney General, California Data Breach Report, February 2016; https://oag.ca.gov/breachreport2016
2. Illinois – Illinois Attorney General, Illinois Information Security and Security Breach Notification Guidance; http://illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guidance.pdf
3. Massachusetts – Massachusetts Office of Consumer Affairs and Business Regulation, A Small Business Guide: Formulating A Comprehensive Written Information Security Program; http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf

F. Court Decisions

1. *Dittman v. UPMC*, No. J-20-2018, 2018 Pa. Lexis 6051(Pa. Nov 21, 2018)
2. *LabMD v. FTC,* No. 16-16270 (11th Cir. June 6, 2018)
3. *FTC v. Wyndham Worldwide Corporation*, 2015 U.S. App. LEXIS 14839; 2015-2 Trade Cas. (CCH) P79,269 (3rd Cir. Aug. 24, 2015);
4. *In re: Sony Gaming Networks and Customer Data Security Breach Litigation*, 2014 BL 15530, (S.D. Cal., No. 3:11-md-02258-AJB-MDD, partially dismissed Jan 21, 2014), at pp. 21-22 (recognizing legal duty to provide security).
5. *Lone Star National Bank v Heartland Payment Systems*, No. 12-20648 (5th Cir, Sept. 3, 2013) (recognizing negligence claim and finding economic loss doctrine not applicable)
6. *Cooney v. Chicago Public Schools*, 2010 Ill. App. LEXIS 1424 (December 30, 2010) (no common law duty to provide security)
7. *Prudential Ins. Co. of Am. v. Dukoff*, No. 07-1080, 2009 U.S. Dist. LEXIS 117843 (E.D.N.Y. December 18, 2009) (must authenticate identity of signer of insurance application in order to enforce signature)
8. *Kerr vs. Dillard Store Services, Inc*., 2009 U.S. Dist. Lexis 11792 (D. Kan. Feb 17, 2009) (electronic signature not enforceable due to lack of security re attribution of signer to signature)

9. *In Re TJX Companies Retail Security Breach Litigation*, 2007 U.S. Dist. Lexis 77236 (D. Mass. October 12, 2007) (rejecting a negligence claim due to the economic loss doctrine, but allowing a negligent misrepresentation claim to proceed)
10. *Wolfe v. MBNA America Bank*, 485 F.Supp.2d 874, 882 (W.D. Tenn. 2007)
11. *Lorraine v. Markel*, 241 F.R.D. 534, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007)
12. *Guin v. Brazos Higher Education Service*, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006)
13. *American Express v. Vinhnee*, 336 B.R. 437; 2005 Bankr. LEXIS 2602 (9th Cir. December 16, 2005).
14. *Bell v. Michigan Council 25*, No. 246684, 2005 Mich. App. LEXIS 353 (Mich. App. Feb. 15, 2005) (Unpublished opinion)
15. *Inquiry Regarding the Entry of Verizon-Maine Into The InterLATA Telephone Market Pursuant To Section 271 of Telecommunication Act of 1996*, Docket No. 2000-849, Maine Public Utilities Commission, 2003 Me. PUC LEXIS 181, April 30, 2003; available at http://www.steptoe.com/assets/attachments/1670.pdf

G. CFPB Decisions and Consent Decrees re Data Security

1. In the Matter of Dwolla, Inc., File No. 2016-CFPB-0007, Consent Order; http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf

H. FTC Decisions and Consent Decrees re Data Security

See list of all FTC Data Security Cases - https://www.ftc.gov/datasecurity

I. European Union

General Data Protection Regulation (GDPR); http://www.eugdpr.org.

K. Other Countries

1. **Argentina**: Act 25,326, Personal Data Protection Act (October 4, 2000), § 9; Security Measures for the Treatment and Maintenance

of the Personal Data Contained in Files, Records, Databanks and Databases, either non state Public and Private (November 2006)

2. **Australia**: Privacy Act 1988, Act No. 119 of 1988 as amended taking into account amendments up to Act No. 86 of 2006, Schedule 3, Clause 4.
3. **Canada**: Personal Information Protection and Electronic Documents Act (2000, c. 5), Schedule 1, § 4.7.; Breach of Security Safeguards Regulations: SOR/2018-64, at http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html
4. **Hong Kong**: Personal Data (Privacy) Ordinance, December 1996, Schedule 1, Principle 4.
5. **Japan**: Act on the Protection of Personal Information, Law No.57, 2003, Articles 20, 21, 22, and 43
6. **South Korea**: The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., Amended by Act No. 7812, December 30, 2005, Articles 28, 29

NOTES

NOTES

7

John Buchanan and Dustin Cho, Covington & Burling LLP, Ch. 17, Internet of Things (IoT): Legal, Policy, and Practical Strategies—When Things Get Hacked: Insurance Coverage for IoT-Related Risks (March 27, 2019)

Submitted by:
Marty Myers

Covington & Burling LLP

This paper was first published by the ABA and released at the Science & Technology (SciTech) Section's Internet of Things (IoT) National Institute on March 27, 2019. Reprinted with permission.

When Things Get Hacked: Insurance Coverage for IoT-Related Risks[1]

John Buchanan and Dustin Cho[2]

I. Introduction

Hackers can do more than steal your data. When they access IoT-connected things—whether household appliances, smart wearables, medical devices, industrial control systems, smart grids, or smart cities—hackers and other bad actors can damage property and endanger lives. As one commentator has put it, "American officials are discovering that in a world in which almost everything is connected—phones, cars, electrical grids, and satellites—everything can be disrupted, if not destroyed."[3]

Reports in recent years highlight some disturbing threat scenarios. Russian government cyber actors have reportedly gained remote access to networks capable of disrupting critical U.S. infrastructure, including the energy sector and the power grid.[4] Cyber soldiers sitting behind

---

1. This paper is adapted from Chapter 17 of *Internet of Things (IoT): Legal, Policy, and Practical Strategies*, a forthcoming ABA publication scheduled for release at the Science & Technology (SciTech) Section's Internet of Things (IoT) National Institute on March 27, 2019.

2. The authors are lawyers in the Washington, D.C. office of Covington & Burling LLP, who represent policyholders exclusively in coverage litigation. The opinions stated in this chapter are those of the authors and should not be attributed either to their law firm or to its clients.

3 David E. Sanger, THE PERFECT WEAPON: WAR, SABOTAGE AND FEAR IN THE CYBER AGE xii (2018)

4. *See, e.g.*, Dep't of Homeland Security & Fed. Bureau of Investigation, Technical Alert 18-074A, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," https://www.us-cert.gov/ncas/alerts/TA18-074A (rev. Mar. 16, 2018) (hereinafter DHS-FBI Alert); Rebecca Smith and Rob Barry, *America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It*, WALL ST. J. (Jan. 10, 2019); *US Warns Public about Attacks on Energy, Industrial Firms*, BUS. INS. (Oct. 23, 2017, 12:30 PM), http://www.businessinsurance.com/article/20171023/NEWS06/912316709/US-warns-public-about-attacks-on-energy,-industrial-firms. These activities are not confined to U.S. infrastructure. *See, e.g., Germany sees big rise in security problems affecting infrastructure*, REUTERS (Feb. 17, 2019), [LINK] ("Germany had learned of 157 hacker attacks on critical infrastructure companies in the second half of 2018 compared to 145 attacks in the whole of the previous year.").

computers in Tehran could open the floodgates on a suburban Westchester County dam.[5] Or the threat could be as banal and close to home as bored teenagers down the street hijacking your "smart" home appliances,[6] or, more ominously, the city's trolley system.[7]

These novel threats arise from what the National Institute of Standards and Technology refers to as "cyber-physical" or "smart" systems, that is, the "co-engineered interacting networks of physical and computational components" that allow the real world and digital world to interact in unprecedented ways.[8] Unfortunately, the cyber-security defenses in many "smart" IoT-connected systems are often . . . not too smart. Hence the reports of hacks on a wide variety of networked IoT devices ranging from smart toilets[9] to drones[10] to medical devices.[11] The federal government's alerts and subsequent security briefings in 2018[12] have raised the general level of awareness of potentially massive physical losses from hacking the IoT or industrial IoT, including attacks on power grids or other networked critical infrastructure.

---

5. Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Ca*se, N.Y. TIMES, (Mar. 23, 2016), https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html.

6. *See* Kashmir Hill, *Here's What It Looks Like When a 'Smart Toilet' Gets Hacked*, FORBES (Aug. 15, 2013), http://www.forbes.com/sites/kashmirhill/2013/08/15/heres-what-it-looks-like-when-a-smart-toilet-gets-hacked-video/.

7. *See* Graeme Baker, *Schoolboy Hacks into City's Tram System*, THE TELEGRAPH (Jan. 11, 2008), http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

8. Cyber-physical systems homepage, Nat'l Inst. of Standards & Tech., http://www.nist.gov/cps/ (last visited Jan. 7, 2018).

9. *See* Hill, *supra* note 6.

10. *See SkyJack: Hacker-Drone That Can Wirelessly Hijack & Control Other Drones*, RT NEWS (Dec. 6, 2013), https://www.rt.com/news/hacker-drone-aircraft-parrot-704/.

11. *See* Tarun Wadhwa, *Yes, You Can Hack a Pacemaker (and Other Medical Devices Too)*, FORBES (Dec. 6, 2012), http://www.forbes.com/sites/singularity/2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too/.

12. DHS-FBI Alert, *supra* note 4; Awareness Briefings: Russian Activity Against Critical Infrastructure, Nat'l Cybersecurity & Commc'ns Integration Ctr (NCCIC), https://share.dhs.gov/p344qjbhqu03/.

These increased warnings of the risk of massive physical losses from cyberattacks naturally raise the question whether that risk can be mitigated by insurance. In fact, a 2015 report titled "Business Blackout," prepared by Lloyd's and Cambridge University, anticipated the types of IoT-related attacks on critical infrastructure that have been the subject of the 2018 federal government warnings, and it analyzed what insurance implications might flow from them.[13] Specifically, the report hypothesized a (now all too plausible) scenario, in which a cyberattack on a utility's industrial control systems disables or destroys multiple power generators in a "smart" grid, resulting in cascading losses throughout the blacked-out power grid and beyond.[14] Such losses could include first-party physical property damage and business-interruption loss for utilities and their customers, third-party property damage and bodily injuries arising from the grid shutdown, and even looting and other social unrest, with accompanying liabilities for the businesses affected.[15]

The cyber insurance market has exploded in recent years; dozens of insurers now offer some kind of cyber coverage.[16] Most cyber-related policies address the intangible losses that accompany network intrusions and data hacks—with a particular focus on privacy-related losses.[17] Thus, while coverage is subject, as always, to the specific (and widely variable)

---

13. Lloyd's Emerging Risk Report, *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid* (May 2015), *available at* http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

14. *Id*. at 11–13.

15. *Id*. at 16–19.

16. *See, e.g.*, Julie Greenwald, *Cyber Insurance Comes of Age*, BUS. INS. (Nov. 6, 2017), http://www.businessinsurance.com/article/20171106/NEWS06/912317022/Cyber-insurance-comes-of-age.

17. *See* Richard S. Betterley, *The Betterley Report: Cyber/Privacy Insurance Market Survey 2018*, 42–69 (June 2018) (charting availability of coverage for various data privacy-related losses under 32 different cyber insurance forms).

wordings of these nonstandard policy forms, if an attack on IoT-connected devices involves conventional data privacy losses, then most available cyber policies can be expected to provide some protection.

But insurance protection for so called cyber-physical risk—the physical losses that may result from the cyber peril of an IoT-related attack—presents a more complex question under many commonly available insurance policies. In fact, most off-the-shelf cyber forms expressly *exclude* coverage for physical bodily injury and property damage.[18] Originally, insurers drafted such exclusions to prevent cyber policies from duplicating the coverage traditionally afforded by standard-form commercial general liability (CGL) and first-party property policies.[19]

But do conventional liability and property policies still clearly cover bodily injury or property damage when it arises from a cyberattack involving IoT devices? This chapter analyzes coverage issues that may arise under traditional CGL and property policies where cyber-physical risks are involved, including the arguments that insurers may raise to escape coverage under such policies and the arguments that policyholders may raise in rebuttal. It then discusses examples of the specialty insurance products that have started to emerge to provide coverage (at a price) for physical harms from cyber perils. It concludes with a few general observations and recommendations for insuring IoT-related risks.

18. *See id.* at 72–75, 88–90 (charting the availability both of first-party coverage for direct damage to equipment and of third-party coverage for bodily injury and property damage).

19. *See infra* note 20.

II. Commercial General Liability Insurance Coverage for Bodily Injury or Property Damage Caused by Cyber Attacks through the IoT

Cyber insurance is now widely available; but as stated above, most cyber policies currently exclude third-party liability coverage for bodily injury and property damage. The explanation commonly provided for this exclusion is that "such losses are covered under CGL . . . policies."[20] But in fact, most recent standard-form CGL policies now incorporate their own cyber-related exclusions—the scope of which is not always clear. This section discusses the evolution of those exclusions and the coverage issues they present in the context of IoT risks.

A. Cyber Exclusions in the CGL Form

Since the turn of this century, the Insurance Services Office (ISO) has repeatedly revised the standard CGL policy's bodily injury and property damage liability coverage part (titled "Coverage A") with respect to cyber-related risks. First, in 2001, the standard CGL policy was revised to state that damage to electronically stored data would not be considered damage to tangible property.[21] Next, in 2004, it was revised to exclude "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic

20. Robert Bregman, *Cyber and Privacy Insurance Coverage*, 37(11) IRMI, THE RISK REPORT 1 (July 2015), ("The [cyber] policies exclude claims alleging bodily injury and property damage because such losses are covered under CGL/property insurance policies.").

21. The 2001 Insurance Services Office CGL policy form added the following two sentences to the definition of "property damage":

> For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

In this form "property damage" is defined as "[p]hysical injury to tangible property, including resulting loss of use of that property," and "[l]oss of use of tangible property that is not physically injured." *See* ISO Properties, Inc., *Commercial General Liability Coverage Form, CG 00 01 10 01* § V.17, at 15 (2000).

data." According to ISO, this new exclusion, "Exclusion p," removed coverage for damage to physical property caused by loss of electronic data.[22] In 2013, a sentence was added to Exclusion p that carved out from the exclusion any "liability for damages because of 'bodily injury.'"[23] That is to say, the new sentence expressly *preserved* coverage for bodily injury arising out of the loss of electronic data.

In May 2014, ISO published two versions of an endorsement that revises Exclusion p: one with a "limited bodily injury exception" and one without.[24] The latter endorsement, in part, reverts to the 2004 variant of Exclusion p—it excludes any damages arising out of the loss of electronic data, regardless of whether the damages are because of bodily injury or property damage.[25] The version with a "limited bodily injury exception" in part adheres to the 2013 edition of Exclusion p, which preserves coverage for damages because of bodily injury.[26]

---

22. *See* ISO Properties, Inc., *Commercial General Liability Coverage Form, CG 00 01 12 04* § I.A.2.p, at 5 (2003). The definition of "electronic data" used in this exclusion was the same as the definition of "electronic data" that the 2001 standard CGL policy had introduced in its definition of "property damage."

23. *See* Insurance Services Office, Inc., *Commercial General Liability Coverage Form, CG 00 01 04 13* § I.A.2.p, at 5 (2012).

24. ISO also published a third version that applies only to Coverage B, the coverage for "personal and advertising injury liability" (thus omitting the revisions to Exclusion p in Coverage A). *See* Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information (Coverage B Only), CG 21 08 05 14* (2013).

25. The "limited bodily injury exception not included" endorsement states in relevant part:

> This insurance does not apply to: . . . Damages arising out of: (1) Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—Limited Bodily Injury Exception Not Included, CG 21 07 05 14* (2013).

26. The "limited bodily injury exception" endorsement states in relevant part:

> This insurance does not apply to: . . . Damages arising out of: (1) Any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health

B. Exclusion p, ¶ (1): "Access to . . . Nonpublic Information"

What was new and identical in both 2014 endorsements was the addition of paragraph (1) of Exclusion p—an exclusion for all damages (whether because of bodily injury or not) arising out of "[a]ny access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information."[27]

In isolation, the undefined terms "access to" and "nonpublic information" are sufficiently vague that an aggressive insurer might argue, for example, that a hospital's or medical device manufacturer's liability for bodily injury caused by alteration of a patient's dialysis machine settings would constitute excluded damages because they arose out of "access to . . . any person's health information or any other type of nonpublic information"; or similarly, that liability for property damage or personal injuries resulting from a hacker's manipulation of the data regulating industrial control systems in a nuclear plant or power grid arose from "access to . . . nonpublic information" and thus is excluded.

In response, insureds would argue that this exclusion, read within its context, cannot reasonably encompass all traditional bodily injury and physical damage caused by hacking of industrial control systems, malicious or negligent alteration of medical device settings, or other

---

> information or any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data. . . . However, unless paragraph (1) above applies, this exclusion does not apply to damages because of 'bodily injury.'

Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—with Limited Bodily Injury Exception, CG 21 06 05 14* (2013).

27. *See* notes 25 and 26.

types of access to nonpublic electronic data regulating networked "things" through the IoT, for at least the following reasons:

- **"Nonpublic Information."** The settings and controls of devices and machinery, though not necessarily accessible to the "public," are not reasonably construed as "any other type of nonpublic information" as contemplated by the exclusion. The interpretive canon of *ejusdem generis*[28] instructs that when a series of items in a list share a certain core characteristic, a "catch-all" term at the end of the list should not be read to stretch beyond what the specifically listed items have in common. In these endorsements, the specifically listed types of "nonpublic information" preceding the catch-all phrase are all traditionally confidential information whose confidentiality is recognized, and protected, by law.[29]

Networked device settings and machine instructions do not generally enjoy either legal or popular recognition as inherently private information. Such data are qualitatively different from the specific categories of protected information listed in paragraph (1) of Exclusion p: "trade secrets, processing methods, customer lists, financial information, credit card information, [and] health information." Under this interpretive principle, therefore, the catch-all term "and any other nonpublic information" in the exclusion endorsements would be read to include other categories of information whose confidentiality is recognized under and protected by the law; but it would not be stretched to encompass a qualitatively different type of "information"—the data regulating electronic control systems.

---

28. "Under the principle of *ejusdem generis*, when a general term follows a specific one, the general term should be understood as a reference to subjects akin to the one with specific enumeration." Norfolk & W. Ry. Co. v. Am. Train Dispatchers Ass'n, 499 U.S. 117, 129 (1991).

29. The exclusion's list of various types of "confidential information" arguably starts after the first term, "patents." While patents are publicly disclosed once granted, they share legal protections similar to those enjoyed by other enumerated types of information such as "trade secrets."

Reinforcing this reading, both endorsements specifically list examples of the damages to which the exclusion applies—all of which are damages associated specifically with data privacy breaches:

> This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of that which is described in Paragraph (1) or (2) above.[30]

All of these types of expense relate to common responses to data breaches, and indeed it is difficult to conceive how the first two items in the list—notification costs and credit monitoring expenses—could arise in the event of traditional physical bodily injury or property damage. This clause's focus on privacy-breach damages reinforces the conclusion that the exclusion was intended only for privacy-related liabilities and not for physical harm that happens to have resulted from a malfunctioning electronic device.

- **"Access To."** Although manipulation of a machine's or device's settings may involve "access to" those settings, the scenarios of concern do not "aris[e] out of" the access to the data that comprises those settings (much less their "disclosure" to the public). Rather, they arise out of the overwriting or overriding of that data—whether intentionally (through hacking) or unintentionally (through user error or a programming bug). In context, damages "arising out of . . . [a]ny access to or disclosure of . . . nonpublic information" means damages arising out of *obtaining* nonpublic information—the damages that typically arise from privacy breaches. When the hacking of industrial control systems or networked devices results in physical harm, by

30. Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—Limited Bodily Injury Exception Not Included, CG 21 07 05 14* (2013); Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—with Limited Bodily Injury Exception, CG 21 06 05 14* (2013).

contrast, the cause is not the *obtaining* of nonpublic information: that is, the prior, correct settings for the machinery or devices in question. Rather, it is the introduction of new instructions that override the original settings. For example, a hacker could alter a dialysis machine's settings even if he could not read the "information" in those settings before he overwrote them. Likewise, a hacker could disrupt a digital signal that provides instructions to a networked device without necessarily receiving or decoding the original intended signal.

In other words, the types of hacking that affect the operations of networked devices do not typically arise out of accessing any *information*—what the exclusion requires. Instead, they arise from someone's access to the *system or location* where the information is stored. What causes the harm is the new, erroneous digital settings or instructions that replace the original settings or instructions. Whether or not those original, correct settings are considered "nonpublic information," the intruder's access to that information is beside the point: the harm arises from the newly introduced malicious information, not from access to the "nonpublic information" itself. Unless the insurer can provide compelling forensic evidence that the essential cause of physical loss was the *release* rather than the *alteration* of confidential information in device settings, the exclusion should not apply.[31]

---

[31] The insurance industry's contemporaneous explanations of Exclusion p are also consistent with a reading that confines the exclusion to data-related, not physical, harm. The memorandum that ISO submitted to regulators in 2013 explaining its adoption of these endorsements states that "damages related to *data breaches, and certain data-related liability*, are not intended to be covered under the abovementioned coverage part. These types of damages may be more appropriately covered under certain stand-alone policies including, for instance, an information security protection policy or a cyber liability policy." Insurance Services Offices, Inc., *Access or Disclosure of Confidential or Personal Information Exclusions Introduced*, Commercial Lines Forms Filing CL-2013-ODBFR, at 7, 8 (2013) (on file with authors) (emphasis added). ISO's statement is consistent with an ISO executive's explanation of the endorsements shortly after they were introduced: he identified other "standalone" ISO insurance products that were available "to provide certain coverage with respect to data breach and access to or disclosure of confidential or personal information," thus suggesting that the new exclusions were intended to dovetail with cyber policies. *See ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INS. J. (July 18, 2014), *available at* http://www.insurancejournal.com/news/east/2014/07/18/332655.htm (quoting Ron Biederman, assistant

C. Exclusion p, ¶ (2): "Loss of . . . Electronic Data"

Paragraph (2) of Exclusion p uses the same language used in CGL policies since 2004 to exclude damages arising out of "[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[32] As noted earlier, since 2014 this exclusion comes in two different versions. The "limited bodily injury exception" version, like the 2013 standard CGL policy, expressly preserves coverage for bodily injury. The other version, like the 2004 standard CGL policy, contains no express carve-out for bodily injury. In both formulations, as with paragraph (1), insurers would likely face a difficult burden to prove that this paragraph (2) exclusion applies to the most common source of cyber-physical loss: physical harms arising from IoT hackers overwriting or overriding the controls of electronic devices.

In sum, Exclusion p in the standard CGL form appears to be aimed at the privacy risks covered under separate cyber policies. But its uncertain application in the context of IoT-related cyber-physical harm may well give rise to highly technical—and no doubt costly—coverage disputes, with the insurer bearing the burden of proving that this exclusion precludes coverage for harm from an IoT attack.

---

vice president, Commercial Casualty at ISO: "As the exposures to data breaches increased over time, standalone policies started to become available in the marketplace to provide certain coverage with respect to data breach and access to or disclosure of confidential or personal information. For instance, ISO Information Security Protection Policy EC 00 10 contains both first and third party coverage through eight separate insuring agreements which address data breach and other cyber-related exposures.").

32. Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—Limited Bodily Injury Exception Not Included, CG 21 07 05 14* (2013); Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—with Limited Bodily Injury Exception, CG 21 06 05 14* (2013).

III. First-Party Property Coverage

Many first-party property policies do not explicitly address coverage for physical harm from a cyberattack.[33] Some, like the ISO's standard "all risks" and "named perils" policies, may not mention cyber-related risks at all in their cause of loss forms.[34] Others may include cyber exclusions targeting only harm to intangible property.

If such a "cyber-silent" policy is an "all risks" policy, meaning it covers losses unless caused by a specifically excluded peril, then coverage for physical damage from a cyberattack should presumptively exist. As one commentator has observed, however, some in the insurance industry assert that standard all risks policies were not created with cyber perils in mind.[35] But an insurer's failure to anticipate a novel risk should not negate the core function of an "all risks" policy; it promises coverage unless an exclusion applies.[36] Without a cyber-specific exclusion to rely on, an insurer facing a claim for physical losses from a cyberattack would likely have to show that the attack fits within some non-cyber-specific exclusion to justify denying coverage.

If a cyber-silent policy is written on a "named perils" basis—meaning it covers only harms from expressly enumerated risks—coverage could still be found in many cases. Under the standard ISO policies, and most others, cyberattacks, as such, are not named perils. Still, they may sometimes fall within the scope of a named peril's definition. For example, the ISO policies

33. *See* Lloyd's Emerging Risk Report, *supra* note 13, at 37.

34. ISO Properties, Inc., *Commercial Property, Causes of Loss—Special Form, CP 10 30 09 17* (2016); ISO Properties, Inc., *Commercial Property, Causes of Loss—Broad Form, CP 10 20 10 12* (2011); ISO Properties, Inc., *Commercial Property, Causes of Loss—Basic Form, CP 10 10 10 12* (2011).

35. *See* Alex Lathrop, *Does Traditional Coverage Apply When Cyber Attacks Cause Physical Damage?*, PROPERTY CASUALTY 360, at 3 (Dec. 29, 2016, 3:00 AM), http://www.propertycasualty360.com/2016/12/29/does-traditional-coverage-apply-when-cyber-attacks?slreturn=1515084401&page=3.

36. *See id.*

name "vandalism" as a covered risk and define it as "willful and malicious damage to, or destruction of," insured property.[37] To be sure, some insurers may balk at coverage under such a provision, asserting that what they meant to cover was only the traditional forms of vandalism, like a brick through a window, not cyber-related perils. But the "vandalism" definition is silent on means and relates only to intent—and many IoT hackers "willfully" or "maliciously" destroy insured property.

Even if a cyberattack does not fit within a named peril's definition, it may result in such a peril—for example, a fire or explosion. In cases where hacking either counts as a named peril or creates such a peril, an insurer would again need to point to a non-cyber exclusion to justify a denial of coverage. This potential exposure to the risk of cyber-physical damage under garden-variety property policies and other traditional policies has been characterized as the "silent cyber risk" that many insurers must evaluate more carefully.[38]

Although many property policies are still silent on cyber risks, some insurers are attempting to exclude them through endorsements or otherwise. For instance, one London Market form common to energy, marine, and industrial property policies, the Institute Cyber Attack Exclusion (CL 380), excludes from coverage any damage "arising from the use or

37. *See* Alex Lathrop & Janine Stanisz, *Hackers Are After More Just Data: Will Your Company's Property Policies Respond When Cyber Attacks Cause Physical Damage and Shut Down Operations?*, 28 ENVTL. CL. J. 286 (2016) (raising the possibility that an attack might count as "vandalism" and analyzing coverage for physical damage from multiple, hypothetical cyberattacks under both all risks and named perils policies).

38. *See, e.g.*, Najiyya Budaly, *Insurers Still Exposed to 'Silent' Cyberrisk Cover, PRA Says*, LAW360 (Jan. 30, 2019) (U.K. Prudential Regulation Authority urges insurers to "review their so-called silent cyber insurance, which opens them up to the risk of acciddntally covering a policyholder against cyber attacks without explicitly agreeing to."), http://www.law360.com/articles/1123619/; Scott Stransky, *Uncovering Silent Cyber Risk*, PROPERTY CASUALTY 360 (July 27, 2017, 8:00 AM), http://www.propertycasualty360.com/2017/07/27/uncovering-silent-cyber-risk; *Insurers Grapple with Cyber-Attacks That Spill over into Physical Damage*, THE ECONOMIST (Dec. 1, 2016), https://www.economist.com/news/finance-and-economics/21711086-only-cyber-calamity-will-reveal-how-ready-industry-insurers-grapple.

operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system."[39] Another London Market form, LMA 3030, excludes from property terrorism insurance "[l]oss or damage by electronic means including but not limited to computer hacking or the introduction of any form of computer virus or corrupting or unauthorised instructions or code or the use of any electromagnetic weapon."[40] These exclusions remain untested in the courts; whether one of them would preclude coverage for the particular circumstances of any given IoT hack may both raise subtle interpretive questions and require a fact-intensive technical analysis.

As new, nonstandard policy wordings proliferate to address the emerging risk of physical property damage from hacking of networked devices, first-party property insurance buyers will increasingly need sharp eyes, and sophisticated coverage advice, to evaluate what protection their policies provide.

IV. Emerging Coverage Solutions

Given the potential for coverage disputes under traditional CGL and property policies, as well as the growing potential for cyber-physical exposures from IoT-connected things, many policyholders may seek purpose-built coverage for risks of physical harm from cyber perils. The market for such products, like the threats they cover, is still evolving. A 2018 market survey of

39. The International Underwriting Association of London, *Institute Cyber Attack Exclusion Clause*, CL 380 (Oct. 11, 2003), *available at* http://www.iuaclauses.co.uk/site/cms/contentDocumentLibraryView.asp?chapter=8&category=57.

40. Lloyd's Market Association, *Terrorism Insurance Physical Loss or Physical Damage Wording*, LMA 3030 (Sept. 1, 2006), *available at* http://www.lmalloyds.com/LMA/Wordings/lma3030.aspx.

cyber insurance products indicates that such coverage options are still confined to a relative handful of insurers.[41]

Nonetheless, the number of insurance products that explicitly cover physical damage from cyber risks can be expected to grow steadily over the next several years. Some signs are already pointing in this direction. As reported in the insurance trade press, FM Global has reported increased inquiries about its products offering cyber-physical coverage;[42] AIG announced in 2017 that it would include cyber coverage in its commercial casualty policies—a move that would likely eliminate Exclusion p and the accompanying coverage issues discussed earlier;[43] and Chubb has introduced an endorsement to address, in part, uncertainty over what happens when a cyber incident creates damage traditionally covered under a property policy.[44] In the United Kingdom, meanwhile, the government-backed terrorism reinsurer, Pool Re, announced in 2017 that it would offer coverage for physical damage from cyberterrorism, following a report on the issue that it produced with the University of Cambridge's Judge

41. *See* Betterley, *supra* note 17, at 88–90 ("Third-party Coverage: Bodily Injury and Property Damage" summary chart).

42. *See* Katie Dwyer, *Cyberattacks Reach the Physical Realm*, RISK & INSURANCE (July 27, 2017), http://riskandinsurance.com/cyberattacks-reach-physical-realm/.

43. *See, e.g.*, Suzanne Barlyn, *AIG to Include Cyber Coverage to Commercial Casualty Insurance*, REUTERS (Oct. 26, 2017), https://www.reuters.com/article/us-aig-cyber/aig-to-include-cyber-coverage-to-commercial-casualty-insurance-idUSKBN1CV2XE.

44. Judy Greenwald, 2017 Innovation Awards: Chubb Global Cyber Facility and Property and Casualty Endorsements, BUS. INS. (Oct. 2, 2017), http://www.businessinsurance.com/article/00010101/NEWS06/912316218/2017-Innovation-Awards-Chubb-Global-Cyber-Facility-and-Property-and-Casualty-En (quoting a Chubb executive as saying, "There are questions, for instance, as to what happens if a cyber incident leads to damage covered by traditional property policies. . . . We don't want uncertainty for our clients.").

Business School.[45] This reinsurance protection may motivate commercial insurers to offer coverage for cyber-physical risks that they may currently attempt to exclude.

These market developments are too numerous, and too fluid, to warrant a comprehensive survey that could become obsolete within a matter of months. But one relatively recent insurance product offers a glimpse into where the market may be heading in response to these novel risks. Global insurance broker Marsh has developed a broad proprietary policy wording, known as Cyber CAT 3.0, crafted to maximize coverage across a range of insurance coverage lines for evolving cyber risks.[46] Cyber CAT 3.0 is specifically promoted as providing "Internet of Things coverage for negligence in the design or manufacture of an IoT product and/or service," as well as coverage for "[p]roperty damage to tangible property caused by a cyber event" and "[b]odily injury and property damage liability resulting from a cyber event."[47]

Policyholders desiring greater contract certainty around cyber-physical risks should consider carefully these new policies and endorsements. Some, like the Marsh form, show promise to prevent the potential coverage disputes identified in this chapter. Over the next decade, as the risk of cyber-physical harm grows more salient, more and more specialty insurance products can be expected to respond to rising market demand for more secure protection against such harms.

---

45. *See* T. Evan, et al., *Cyber Terrorism: Assessment of the Threat to Insurance; Cambridge Risk Framework Series*, Centre for Risk Studies, University of Cambridge (Nov. 2017).

46. *See Cyber Cat 3.0 Fact Sheet*, MARSH, *available at* https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Cyber%20CAT%203.0%20Fact%20Sheet%20Final%20Spring%202018.pdf.

47. *Id.* at 2.

V. Conclusions and Recommendations for Entities with IoT Risk Exposures

Both insurers and insureds are confronting a relatively novel set of risks: old-fashioned physical harms arising from newfangled cyber perils. Many insureds confronted with these cyber-physical losses will argue that they should be covered under their conventional all-risk general liability and first-party property policies. Some insurer-side claims handlers may look for reasons why these risks should fall outside the policy terms.

To address these new issues, insurance purchasers would be well advised to take the following steps:

- **Understand the cyber-physical risks involved.** This means surveying the industrial control systems and other networked "smart" devices that the insured either manufactures or uses in its own operations; hardening the cybersecurity of those systems and devices; and thinking through the potential consequences of a cybersecurity failure.

- **Understand how all policy language will respond to those risks.** This means at a minimum analyzing the policy terms under cyber, technology errors and omissions, general liability, property and any other potentially applicable lines of coverage, such as kidnap and ransom policies and even directors and officers policies. Do the "dovetailing" exclusions actually dovetail? Or do they leave gaps—whether because they contemplate protection from another line of coverage that in fact has a reciprocal exclusion, or merely because the coverage grant in one line fails to align intelligently with the exclusion in another?

- **If possible, plug the gaps and clarify the coverage grants.** To clarify coverage specifically for cyber-physical risks, insurance buyers may request changes in their existing lines of coverage or explore the purchase of specialty coverage solutions.

- **Expect disputes.** They are virtually inevitable at the claims stage with any previously unrecognized or underestimated risk. But attention to both the big picture and the nitty-gritty details at the underwriting stage should reduce the chances that IoT-related risks and cyber-physical losses will generate the next big wave of coverage litigation.

NOTES

NOTES

8

Hunton Andrews Kurth Client Alert, SEC Publishes New Guidance on Public Company Cybersecurity Disclosure (February 2018)

Submitted by:
Lisa J. Sotto
Aaron P. Simpson

Hunton Andrews Kurth LLP

Client Alert

February 2018

SEC Publishes New Guidance on Public Company Cybersecurity Disclosure

The US Securities and Exchange Commission (SEC) published long-awaited cybersecurity interpretive guidance for public companies on February 21, 2018. The new interpretive guidance, while not revolutionary, marks the first time that the five SEC commissioners, as opposed to agency staff, have provided official agency guidance to public companies regarding their cybersecurity disclosure and compliance obligations. The guidance reiterates public companies' obligation to disclose material information to investors, particularly when that information concerns cybersecurity risks or incidents. It also addresses two topics not previously addressed by agency staff: the importance of cybersecurity policies and procedures in the context of disclosure controls, and the application of insider trading prohibitions in the cybersecurity context.

Key Points

As detailed below, the new guidance focuses on several key points that we believe reflect learnings from the SEC's recent experiences regarding both the Division of Enforcement's investigations of public companies involved in cyber events and the Division of Corporation Finance's ongoing disclosure reviews of registration statements and periodic filings. Central to the guidance are the following themes:

- Crucial to a public company's ability to make required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact such matters may have on the company, as well as a protocol to determine the potential materiality of the risks and incidents.
- Development of effective disclosure controls and procedures is best achieved when a company's directors, officers and others responsible for developing and overseeing the controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face.
- The SEC is concerned about potential insider trading around cyber events, and companies should scrutinize their compliance policies to ensure that such activity is sufficiently addressed.
- In light of the guidance's discussion concerning the potential materiality of cybersecurity, companies should consider whether they need to revisit or refresh previous disclosures made to investors.

Background

The SEC introduced the guidance by observing that "cybersecurity risks pose grave threats to investors, our capital markets, and our country." The guidance notes the rapidly evolving technological landscape in which modern public companies operate, then catalogs a series of costs and other negative consequences that companies falling victim to cyberattacks may suffer:

- remediation costs, such as liability for stolen assets or information, repairs of system damage and incentives to customers or business partners in an effort to maintain relationships after an attack;
- increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees and engaging third-party experts and consultants;
- lost revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-US authorities;
- increased insurance premiums;
- reputational damage that adversely affects customer or investor confidence; and
- damage to the company's competitiveness, stock price and long-term shareholder value.

Given the frequency, magnitude and cost of cybersecurity incidents, the SEC expresses its belief that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion. In doing so, the SEC notes that this requirement applies not just to companies that have suffered a cyber incident, but also to those that are subject to material cybersecurity risks but may not yet have been the target of a cyberattack.

Materiality of Cybersecurity Disclosure

The new guidance provides a number of pointers as to how a public company should undertake a materiality analysis in the context of a cybersecurity risk or incident. In determining their disclosure obligations, the guidance notes that companies should generally weigh, among other factors, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The SEC emphasizes that the materiality of cybersecurity risks or incidents depends upon their nature, extent and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm such incidents could cause. According to the SEC, such harm could include damage to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state, federal and foreign governmental authorities.

The guidance further emphasizes that public companies are not expected to publicly disclose specific, technical information about their cybersecurity systems, nor are they required to disclose potential system vulnerabilities in such detail as to empower threat actors to gain unauthorized access. Moreover, the SEC recognizes that a company may require time to gather the material facts related to a cybersecurity incident before making appropriate disclosure. The SEC also notes that while it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding an incident, the existence of an ongoing internal or external investigation does not on its own provide a basis for avoiding disclosures of a material cybersecurity incident. Likewise, the SEC expects that when a company becomes aware of a cybersecurity risk or incident that would be material to investors, the company should make appropriate disclosure prior to the offer and sale of securities. It should also take steps to prevent insiders from trading in its securities until investors have been appropriately informed about the risk or incident. Notably, the SEC did not impose a Form 8-K reporting obligation regarding cyber events.

Additionally, the guidance provides insight into the SEC's views on the duty to correct and the duty to update in the context of cyber disclosure. The guidance reminds companies that they may have a duty to correct prior disclosure that the company later determines was untrue (or if it omitted a material fact) at the time it was made, such as when a company subsequently discovers contradictory information that existed at the time of the initial disclosure. Likewise, companies may have a duty to update disclosure that becomes materially inaccurate after it is made, such as when an erroneous original statement is still being relied on by investors. Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident. As always, the SEC eschews boilerplate disclosures and reminds companies to provide information specifically tailored for their own circumstances.

Risk Factors

The guidance urges companies to consider the following cyber risk factors, among others:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks;
- the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;
- the potential for reputational harm;
- existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and
- litigation, regulatory investigation and remediation costs associated with cybersecurity incidents.

Elaborating further, the SEC notes that companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. For example, the SEC posits that if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident "may" occur. Instead, the SEC believes the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose specific risks to the company's business and operations.

MD&A

In preparing MD&A disclosure, the SEC reminds companies that the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents and the risks of potential cybersecurity incidents, among other matters, may be relevant to the company's analysis. In addition, companies should consider the need to discuss the various costs associated with cybersecurity issues, including:

- loss of intellectual property;
- the immediate costs of an incident, as well as the costs associated with implementing preventative measures;
- maintaining insurance;
- responding to litigation and regulatory investigations;
- preparing for and complying with proposed or current legislation;
- engaging in remediation efforts;
- addressing harm to reputation; and
- the loss of competitive advantage that may result.

Description of Business

Regarding Item 101 of Regulation S-K, the SEC reminds companies that if cybersecurity incidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company should provide appropriate disclosure around those issues.

Legal Proceedings

In preparing disclosures under Item 103 of Regulation S-K, the SEC observes that material legal proceedings may include those related to cybersecurity issues. By way of example, the SEC indicates that if a company experiences a cybersecurity incident involving the theft of customer information and the incident results in material litigation by customers against the company, the company should describe the litigation, including the name of the court in which the proceedings are pending, the date the proceedings are instituted, the principal parties, a description of the factual basis alleged to underlie the litigation and the relief sought.

Financial Statement Disclosure

The new guidance provides several examples of how cybersecurity risks and incidents may affect a company's financial statements, including:

- expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services;
- loss of revenue, providing customers with incentives, or a loss of customer relationship assets value;
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties and insurance premium increases; and
- diminished future cash flows; impairment of intellectual, intangible or other assets; recognition of liabilities; or increased financing costs.

In this regard, the SEC expects that a company's financial reporting and control systems would be designed to provide reasonable assurance that information about the range and magnitude of the

financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.

Board Risk Oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure. To the extent cybersecurity risks are material to a company's business, the SEC believes this discussion should include the nature of the board's role in overseeing the management of that risk. Additionally, the SEC believes disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues will allow investors to assess how a board of directors is discharging its risk oversight responsibility.

Disclosure Controls and Procedures

The guidance encourages public companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. To that end, the SEC urges companies to assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.

When designing and evaluating disclosure controls and procedures, the SEC reminds companies they should consider whether such controls and procedures will appropriately record, process, summarize and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors and make timely disclosures regarding such risks and incidents.

When a company's principal executive officer and principal financial officer make required certifications under Exchange Act Rules 13a-14 and 15d-14 regarding the design and effectiveness of disclosure controls and procedures, the SEC notes that management should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

Insider Trading

Perhaps in response to several recent events involving allegations of insider trading around cyber incidents that received significant media coverage, the new guidance also provides direction on insider trading law as it relates to information about cybersecurity risks and incidents, including vulnerabilities and breaches. Put simply, the SEC is of the view that information about a company's cybersecurity risks and incidents may be material nonpublic information, and the SEC believes that directors, officers and other corporate insiders would violate the antifraud provisions of the federal securities laws if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.

The guidance encourages companies to consider how their codes of ethics and insider trading policies take into account and seek to prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. In this respect, the SEC believes that it is important to have well-designed policies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents.

In addition, while companies are investigating and assessing significant cybersecurity incidents, and determining the underlying facts, ramifications and materiality of these incidents, the SEC urges them to consider whether and when it may be appropriate to implement restrictions on insider trading in their securities. The SEC favors insider trading policies and procedures that include prophylactic measures designed to prevent directors, officers and other corporate insiders from trading on the basis of material nonpublic information before public disclosure of the cybersecurity incident. The SEC also believes that companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure.

Regulation FD

The guidance concludes with a reminder that public companies are prohibited in many circumstances from making selective disclosure about cybersecurity matters under SEC Regulation FD. Again, the SEC expects companies to have policies and procedures to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made in a manner otherwise compliant with the requirements of that regulation.

Commissioner Stein's Public Statement

The new guidance is perhaps most notable for the issues it does not address. In a statement issued coincident with the release of the new guidance, Commissioner Kara Stein expressed disappointment that the new guidance did not go further and highlighted four areas where she would have preferred the SEC to have sought public comment in connection with commencing rulemaking. These areas concern:

- rules that address improvements to the board's risk management framework related to cyber risks and threats;
- minimum standards to protect the personally identifiable information of investors and whether such standards should be required for key market participants, such as broker-dealers, investment advisers and transfer agents;
- rules that would require a public company to provide notice to investors (e.g., a Current Report on Form 8-K) in an appropriate time frame following a cyberattack and to provide disclosure that is useful to investors, without harming the company competitively; and
- rules that are more programmatic and that would require a public company to develop and implement cybersecurity-related policies and procedures beyond merely disclosure.

Final Takeaways

Because the SEC cannot legally use interpretive guidance to announce new law or policy—the Administrative Procedure Act still requires public notice and comment for any rulemaking—the guidance is evolutionary, rather than revolutionary. Still, it consolidates into a single document the SEC's latest thinking on this important issue, and spares public companies the need to sift through prior staff

interpretive guidance,[1] staff speeches and publicly available staff comment letters to divine the agency's views on these issues. The guidance signals a number of areas where the SEC expects companies to enhance their compliance policies and procedures, such as those regarding disclosure controls and insider trading. Now is a good time for public companies to begin that review. Companies also should consider whether their current cybersecurity disclosures are consistent with the many topics the guidance addresses.

Given the intense public and political interest in cybersecurity disclosure by public companies, we anticipate that this latest guidance will not be the SEC's final word on this critical issue. Indeed, the SEC noted that the commissioners and staff continue to monitor cybersecurity disclosures carefully.

The new guidance makes clear that the SEC "continues to consider other means of promoting appropriate disclosure of cyber incidents." The SEC has not yet brought a significant enforcement action against a public company due to perceived deficiencies in cybersecurity disclosure. With the release of the new guidance and the clarification of the SEC's views on these issues, companies are also now on notice as to what the agency's Division of Enforcement will expect.

Contacts

Lisa J. Sotto
lsotto@huntonAK.com

Scott H. Kimpel
skimpel@huntonAK.com

Matthew P. Bosher
mbosher@huntonAK.com

Aaron P. Simpson
asimpson@huntonAK.com

W. Lake Taylor Jr.
tlake@huntonAK.com

Paul M. Tiao
ptiao@huntonAK.com

Brittany M. Bacon
bbacon@huntonAK.com

**As of April 1, 2018, Hunton & Williams is now Hunton Andrews Kurth.*

[1] The SEC staff has not as of yet taken steps to withdraw the Division of Corporation Finance's CF Disclosure Guidance: Topic No. 2 — Cybersecurity, issued in 2011, though its content is largely subsumed into this new guidance. Rules and interpretive materials issued by other SEC offices and divisions with respect to other regulated entities (e.g., broker-dealers or investment advisers) is unaffected by the new guidance.

NOTES

9

A How-To Guide to Information Security Breaches, BNA, Inc., Privacy & Security Law Report, Vol. 6, No. 14, pp. 559–562 (April 2, 2007)

Lisa J. Sotto
Aaron P. Simpson

Hunton Andrews Kurth LLP

BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Since 2005, there have been reports of over 500 U.S. security breaches. Proactive incident response planning can help minimize the impact when and if a breach occurs. The authors provide advice on responding to and managing a data breach, including information on state law variations, relevant stakeholders, and tips on actual notification.

A How-To Guide to Information Security Breaches

BY LISA J. SOTTO AND AARON P. SIMPSON

Contrary to what the headlines suggest, information security breaches are not a new phenomena. What is new is that we are hearing about them in record numbers. While consumers are newly focused on information security due to the emergence of e-commerce, the reason security breaches now seem ubiquitous is a result of the development of a body of state laws requiring companies to notify affected individuals in the event of a breach. The differing requirements of over 35 state security breach notification laws make legal compliance a challenge for organizations operating on a national level.

Lisa Sotto heads the Privacy and Information Management Practice at Hunton & Williams LLP and is a partner in the New York office. She is also vice chairperson of the DHS Data Privacy and Integrity Advisory Committee. Sotto may be contacted at lsotto@hunton.com. Aaron P. Simpson is an associate in the Privacy and Information Management Practice at Hunton & Williams, New York. He may be contacted at asimpson@hunton.com.

Background

Since 2005, there have been reports of over 500 security breaches, many of which have involved the most respected organizations in the United States.[1] In fact, the number of reported incidents does not begin to define the actual number of breaches that have occurred in the United States during the past two years. From universities to government agencies to Fortune 500 companies, no industry sector has been spared. These breaches have run the gamut from lost backup tapes and laptops, to hacking incidents, to organized crime. The reported breaches are estimated to have exposed personal information contained in over 100 million records. Consequently, a significant percentage of the American public has received notification that the security of their personal information has been breached. Indeed, it seems that hardly a day goes by without a new press report of a significant security breach.

[1] *See* Privacy Rights Clearinghouse, "A Chronology of Data Breaches," available at http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited March 27, 2007).

 ISSN 1538-3423

State Security Breach Notification Laws

Public awareness was not focused in earnest on security breaches until 2005, fully two years after California enacted a law requiring organizations to notify affected Californians of a security breach.[2] At the time of enactment, few understood the enormous implications of that law. Since 2005, 35 other states, as well as New York City, Washington, D.C. and Puerto Rico, have jumped on the bandwagon and enacted breach notification laws of their own. In addition, numerous federal security breach bills have been proposed. With no clear frontrunner, it is hard to predict when a federal law might be passed, thought a federal preemptive law appears likely.

At the state level, the duty to notify individuals affected by a breach generally arises when there is a reasonable belief that unencrypted, computerized sensitive personal information has been acquired or accessed by an unauthorized person. Typically, the state laws define ''personal information'' to include an individual's first name or first initial and last name, combined with one of the three following data elements:

- Social Security number;
- driver's license or state identification card number, or
- financial account, credit or debit card number, along with a required password or access code.

Unfortunately, entities struggling with a potential breach must look beyond the language of the ''typical'' state law in the event of a national, or even multi-state, incident. The variations among state breach notification laws greatly complicates the legal analysis as to whether the breach laws are triggered with respect to a particular event. Because most breaches impact individuals in multiple jurisdictions, companies often must take a ''highest common denominator'' approach to achieve legal compliance.

Key areas of variation among state breach notification laws include:

- *Affected Media*: Under most state breach laws, notification is required only if ''computerized'' data has been accessed or acquired by an unauthorized individual. In some states, however, including North Carolina, Hawaii, Indiana and Wisconsin, organizations that suffer breaches involving paper records are required to notify affected individuals.
- *Definition of ''Personal Information''*: Breach notification laws in some states expand the definition of personal information to include data elements such as medical information (Arkansas, Puerto Rico), biometric data (Nebraska, North Carolina, Wisconsin), digital signatures (North Carolina, North Dakota), date of birth (North Dakota), employee identification number (North Dakota), mother's maiden name (North Dakota), and tribal identification card numbers (Wyoming).
- *Notification to State Agencies*: Many states require entities that have suffered a breach to notify state agencies. Currently, the states that require such notification include Hawaii, Maine, New Hampshire, New Jersey, New York, North Carolina and Puerto Rico. In Puerto Rico, organizations must notify the state government within ten days of detecting a breach. In New Jersey, the breach notification law requires entities to notify the state police prior to notifying affected individuals.
- *Notification to Credit Reporting Agencies*: While the threshold for notification differs among the state laws, many states require organizations that suffer a breach to notify the three national consumer reporting agencies (Equifax, Experian and Transunion). Among the states with this requirement, the state with the lowest threshold requires notification to the credit reporting agencies in the event 500 state residents must be notified in accordance with the notification requirement.
- *Timing of Notification to Affected Individuals*: Most state notification laws require notification to affected individuals within ''the most expedient time possible and without unreasonable delay.'' Some states, such as Ohio, Florida and Wisconsin, require notification within 45 days of discovering the breach.
- *Harm Threshold*: Some states (*e.g.*, Indiana, Michigan, Ohio, Rhode Island, Utah and Wisconsin) require notification of affected individuals only if there is a reasonable possibility of identity theft. Other states (*e.g.*, Colorado, Idaho, Kansas, Maine, New Hampshire, New Jersey and Vermont) do not require notification unless it has been determined that misuse of the information has occurred or is reasonably likely to occur. And in other states (*e.g.*, Arkansas, Florida, Hawaii and Louisiana) notification is not required unless there is a reasonable likelihood of harm to customers. For organizations that suffer multi-state security breaches, any harm threshold is irrelevant as a practical matter because many state breach notification laws do not contain such a threshold.

Federal Enforcement

In addition to the compliance maze at the state level, the Federal Trade Commission (FTC) has enforcement authority in the privacy arena pursuant to Section 5 of the FTC Act.[3] Section 5 of the FTC Act prohibits unfair or deceptive trade practices. The FTC recently has brought a number of enforcement actions pursuant to Section 5 stemming from security breaches. In fact, most of the enforcement actions brought by the FTC in the privacy arena have resulted from security issues. Some of the more noteworthy FTC enforcement actions stemming from security breaches have included those against BJ's Wholesale Club, CardSystems, ChoicePoint and DSW.

The CardSystems case highlights the significant reputational risk associated with privacy events generally, and security breaches in particular. In this case, over 40 million credit and debit card holders' information was accessed by hackers leading to millions of dollars in fraudulent purchases. In its enforcement action, the FTC alleged that the company's failure to take appropriate action to protect personal information about millions of consumers was tantamount to an unfair trade practice. As part of its settlement with the FTC, CardSystems agreed to implement a comprehensive information security program and conduct audits of the program biennially for 20 years. The real punishment, however, was the reputational damage the company suffered in the wake of the breach. Both Visa and Discover severed their relationship with CardSystems and

[2] Cal. Civ. Code § 1798.82 (2006).

[3] 15 U.S.C. § 45 (2005).

  PVLR ISSN 1538-3423

the company ultimately was sold to an electronic payment company in Silicon Valley.

As our society becomes increasingly information-dependent, it is likely that there will be an increase in FTC enforcement associated with security breaches. In fact, in response to heightened consumer concern and an increased need for regulatory oversight in this arena, the FTC recently established a new division of Privacy and Identity Protection. This signals a new FTC focus on data privacy and security, along with what will likely be a concomitant increase in enforcement.

Managing a Data Breach

If a possible breach occurs, it is critical to determine as quickly as possible whether the event triggers a requirement to notify affected individuals. To make this determination, organizations must be able to answer the following questions:

1. *What information was involved?* Does the compromised information meet the definition of ''personal information'' under any of the state breach notification laws? As discussed above, certain states have adopted expansive definitions of ''personal information'' for purposes of their breach notification laws. These broader definitions must be considered in analyzing the information involved in the event.
2. *Was the information computerized?* In most states, only incidents involving computerized information require individual notification. But special attention should be paid to the laws in those states in which notification is required for incidents involving personal information in any form, including paper.
3. *Was the information encrypted?* Encryption is available as a safe harbor under every extant state security breach notification law. Importantly, all of the relevant laws are technology-neutral, meaning they do not prescribe specific encryption technology. If the information is maintained in an unreadable format, then it may be considered encrypted for purposes of the state breach laws. Encryption does not, however, include password-protection on equipment such as desktop computers, laptop computers and portable storage devices. As a result, many organizations have been required to notify affected individuals when laptop computers subject to password-protection have been lost or stolen.
4. *Is there a reasonable belief that personal information was accessed or acquired by an unauthorized person?* If an entity has a reasonable belief that the information was compromised by an unauthorized person, notification is required. Note that a number of state breach notification laws contain a harm threshold whereby notification is not required unless there is reasonable possibility of harm, misuse or identity theft (*see above*). Organizations should be wary of relying on harm thresholds, however, because they are not included in many state breach laws and thus may not be available in the event of a multi-state breach.

Because breaches come in all shapes and sizes, many of them require significant technical analysis to answer these questions. Organizations often must enlist the assistance of highly skilled forensic investigators to assist with the evaluation of their systems.

Recognize the Stakeholders

Once an organization has determined that the breach notification laws have been triggered, it is important to understand the panoply of stakeholders throughout the breach process. Depending on the type of organization involved, the potential universe of stakeholders is extensive and may include:

- *Affected individuals*: Individuals affected by a security breach are the primary focus for every organization during the notification process. Although the breach may not have occurred as a result of any misdeeds by the organization suffering the breach, in the eyes of consumers, employees and other affected individuals, the organization is responsible for the data it collects and maintains. As a result, regardless of the circumstances, an organization suffering a security breach should be appropriately helpful and respectful to individuals whose data may have been compromised.
- *Board of Directors/Senior Management*: Information security is no longer an area of a company that is relegated to the dusty basement. Front-page headlines and stock drops stemming from early security breaches made sure of that. It is often advisable to involve the Board of Directors (or its equivalent) and senior management soon after learning of a security breach affecting the organization.
- *Law Enforcement*: Depending on the nature of the event, it may be important to report the security breach to law enforcement authorities for purposes of conducting an investigation. The state security breach laws allow organizations to delay notifying affected individuals pending a law enforcement investigation. New Jersey's breach notification law makes it a legal requirement to notify law enforcement prior to notifying affected individuals.
- *State and Federal Regulators*: In addition to the laws' requirements to notify state regulators, organizations should give serious consideration to notifying the FTC in the event of a significant security breach. Proactively notifying the FTC, while not a legal requirement, provides an organization with the opportunity to frame the circumstances of the breach and provide appropriate context. Because the FTC will undoubtedly learn about every significant security breach, organizations are well-advised to tell the story themselves rather than have the FTC learn about the breach from unfavorable media reports.
- *Financial Markets*: For publicly-traded companies, some security breaches rise to the level of reportable events. In these cases, it may be necessary to notify the Securities and Exchange Commission and the relevant exchange of the breach.
- *Payment Card Issuers*: To the extent payment cards are involved, it is often essential to consult the card issuers as early as possible in the process. Organizations should review their contractual obligations with the card issuers because there are likely to be provisions relevant to a security breach. In addition, the card issuers may require organizations suffering breaches to file formal incident reports. Depending on the scope of the breach, the card issuers also may require that an

independent audit be conducted by their own auditors.

- *Employees*: In some cases, employees of the organization should be notified of an incident affecting customers. Many employees care deeply about the entity for which they work. To the extent the organization's reputation may be tarnished by the event, employees will not want to be left in the dark about the incident.
- *Shareholders*: Public companies that suffer breaches must consider their shareholders in the aftermath of a breach. The investor relations department should be mobilized in the event of a significant breach to respond to investors' concerns.
- *Auditors*: In some cases, security breaches may need to be reported to a company's auditors.
- *Public*: Security breaches often ignite the passions of the public at-large. In managing the process of notification, organizations should give careful consideration to the anticipated public response to the incident. In many cases, it is helpful to work with experienced public relations consultants. The risk to an organization's reputation stemming from a security breach far exceeds the risk associated with legal compliance. Thus, it is imperative in responding to a security breach to consider measures that will mitigate the harm to an organization's reputation.

Timing of Notification

Once the extent and scope of the incident have been defined and it is determined that notification is required, the next step is to notify affected individuals. Most state security breach laws require organizations that suffer a breach to notify affected individuals ''in the most expedient time possible and without unreasonable delay.'' In several states, notification is required within 45 days of the date the incident was discovered. Under both timeframes, the date of actual notification may be delayed by the exceptions available in most states for law enforcement investigations and restoring system security.

Pursuant to the law enforcement exception, notification may be delayed if a law enforcement agency determines that notification would impede a criminal investigation. Thus, if law enforcement has requested such a delay, the clock does not start ticking on notification until after the agency determines that notification will not compromise the investigation.

As to the exception for restoring system security, notification to affected individuals may be delayed to provide the affected organization time to take any security measures that are necessary to determine the scope of the breach and to restore the ''reasonable integrity of the system.'' Organizations should not take this exception lightly—notification to consumers of a system vulnerability may tip off copycat fraudsters to a system weakness they can exploit. Thus, prior to notifying affected individuals, it is essential for organizations suffering security breaches to restore the integrity of their systems.

Entities that rely on either the law enforcement or system security exception should document such reliance. In Hawaii, such documentation is a legal requirement.

Notification to Individuals

Letters to individuals notifying them of a possible compromise of their personal information should be simple, free of jargon and written in plain English. Entities would be well-advised to avoid legalistic phrases and any attempt to pin blame elsewhere. Organizations that have been most favorably reviewed by individuals following a breach are those that have accepted responsibility and provided useful information to recipients. (A breach notification letter is not the place for marketing!)

Organizations should keep in mind that, in addition to impacted individuals, the notification letter will likely be scrutinized by numerous interested parties, including regulators, plaintiffs' lawyers and the media. As a result, it is essential to strike the appropriate tone while at the same time providing a meaningful amount of substance.

There is a growing de facto standard, depending on the information breached, for the types of ''offerings'' companies are making to affected individuals in their notice letters. These offerings typically include:

- *Credit Monitoring*: In the event a Social Security number or some other form of identification that may contain a Social Security number (such as a driver's license number or a military identification card number) has been compromised, it has become standard to offer affected individuals one year of credit monitoring services. Depending on the size of the breach, this can be a significant cost for companies.
- *Free Credit Report*: Separate and apart from credit monitoring, organizations should inform affected U.S. individuals that they are entitled to one free credit report annually from each of the three national credit reporting agencies.
- *Fraud Alert*: Organizations also may want to recommend that affected individuals place a fraud alert on their credit file for additional protection. There is no charge for this service. Because fraud alerts can have a significant impact on a consumer's day-to-day purchase habits, most organizations simply suggest to consumers that this is an option rather than insist they take such action.

In addition to the standard offerings, the letter should describe the details of the security breach. For obvious reasons, these details should never include the specific affected payment card or Social Security numbers impacted by the breach. Instead of providing this detail, it is most effective to explain what happened and what the organization is doing to help individuals affected by the breach. In many cases, this means providing the individual with information about credit monitoring and other information about how they may protect themselves. Also, it may be necessary to establish a call center (with trained agents) to handle consumer response to the incident.

As a general rule, if an organization is required to notify in a few jurisdictions, it is recommended that it notify in all jurisdictions (often this includes foreign countries). With few exceptions, this has become standard in the privacy realm. A few companies that suffered early security breaches after California passed its law were torched by the media and subjected to severe criticism by irate state attorneys general for notifying affected Californians but not affected residents of other states without breach notification laws. The collective experi-

  PVLR ISSN 1538-3423

ence of these companies highlights an important, but often misunderstood, concept: technical compliance with law is necessary but not sufficient in the privacy arena. Privacy events are hot button social issues that often transcend mere legal compliance. Indeed, the risk to an organization's reputation and revenues often far exceeds the risk associated with non-compliance with breach laws. As a result, organizations responding to a breach should focus on doing the right thing as opposed to doing only those things that are required by law.

Lessons Learned

Security breach notification laws have brought information security issues into the spotlight. While no information security is perfect, proactive incident response planning can help minimize the impact when and if a breach occurs. Such planning includes inventorying the entity's databases that contain sensitive personal information, understanding how sensitive personal information flows through the organization, conducting ongoing risk assessments for internal and external risk to the data and responding to reasonably foreseeable risks, maintaining a comprehensive written information security program, and developing a breach response procedure. Given that a recent survey of 31 breaches ranging in size from 2,500 records to 263,000 records conducted by the Ponemon Institute found that the average cost of responding to a security breach was $182 per lost customer record with an average total cost of $4.8 million, the stakes are higher than ever for companies to focus on their information security programs.[4] Most importantly, concern and respect for information security should be integrated into the organization's core values. A breach response plan alone, without demonstrable organizational concern for information security generally, exposes the organization to significant risk. With the stakes as high as they are, all organizations should be taking a closer look at their information security practices.

[4] *See* Ponemon Institute, ''2006 Annual Study: Cost of a Data Breach'' (October 2006).

NOTES

10

Aaron P. Simpson and Adam H. Solomon, Dealmakers Ignore Cyber Risks at Their Own Peril, Pratt's Privacy & Security Law Report, Vol. 1, No. 2, pp. 46–52 (October 2015)

Submitted by:
Lisa J. Sotto
Aaron P. Simpson

Hunton Andrews Kurth LLP

AN A.S. PRATT PUBLICATION
OCTOBER 2015
VOL. 1 N

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

EDITOR'S NOTE: COMBATING RISKS
Steven A. Meyerowitz

DEALMAKERS IGNORE CYBER RISKS AT THEIR OWN PERIL
Aaron P. Simpson and Adam H. Solomon

CYBERSECURITY AND GOVERNMENT "HELP" – ENGAGING WITH DOJ, DHS, FBI, SECRET SERVICE, AND REGULATORS – PART I
Alan Charles Raul and Tasha D. Manoranjan

THE DEFEND TRADE SECRETS ACT OF 2015: ATTEMPTING TO MAKE A FEDERAL CASE OUT OF TRADE SECRET THEFT – PART I
David R. Fertig, Christopher J. Cox, and John A. Stratford

FTC LAUNCHES "START WITH SECURITY" INITIATIVE: RELEASES DATA SECURITY GUIDANCE AND ANNOUNCES NATIONWIDE CONFERENCE SERIES
James S. Talbot

FFIEC RELEASES VOLUNTARY CYBERSECURITY ASSESSMENT TOOL
James S. Talbot and Cristina Vasile

JEEP HACK DRIVES CYBER, CRISIS, LIABILITY, AND SUPPLY CHAIN COVERAGE ISSUES
Joseph F. Bermudez

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT
OCTOBER 2015 || VOL. 1 • NO. 2

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Aaron P. Simpson and Adam H. Solomon, *Dealmakers Ignore Cyber Risks at Their Own Peril*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [46] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2015–Pub. 4939)

Dealmakers Ignore Cyber Risks at Their Own Peril

By Aaron P. Simpson and Adam H. Solomon*

With cyber attacks pervasive in commerce today, it is imperative for businesses engaging in corporate transactions to consider the cybersecurity and privacy risks of their investments prior to purchasing, merging with, or financing a company. Dealmakers can mitigate these risks and prevent the incurrence of unanticipated costs and criticism from unforeseen information security and privacy issues that may emerge after the closing of a deal through thoughtful due diligence efforts. The authors of this article discuss the cybersecurity and privacy due diligence process.

In today's commercial environment, it is imperative for businesses engaging in corporate transactions to consider the cybersecurity and privacy risks of their investments prior to purchasing, merging with or financing a company. Cyber attacks across industry are rampant, and purchasers face significant risks of data breaches and privacy violations occurring before or arising after the closing of a deal. These events can increase liability and ultimately harm the value of the investment. Through thoughtful due diligence efforts, dealmakers can mitigate these risks and prevent the incurrence of unanticipated costs and criticism from unforeseen information security and privacy issues that may emerge after the closing of a deal.

There are many liabilities that may arise from the collection, use, disclosure and security of company data. The most significant liabilities result from cyber attacks compromising sensitive information maintained by the company. As a starting point, companies experiencing a breach incur potentially hefty costs investigating, remediating and responding to breaches, including the cost of conducting a forensic examination and fixing, rebuilding, upgrading or altogether replacing impacted computer systems. On top of these expenses, data breaches pose liability risks associated with regulatory enforcement, fines and assessments levied by payment card brands or regulators, private litigation such as consumer class actions and shareholder derivative suits and congressional inquiries, as well as losses of sales, goodwill, intellectual property, information assets and shareholder value. Similar liability risks may arise for companies in data-intensive fields from the use of consumer information in violation of privacy laws or company privacy policies that are treated as actionable public representations under state and federal consumer protection laws.

---

* Aaron P. Simpson, a member of the Board of Editors of *Pratt's Privacy & Cybersecurity Law Report*, is a partner at Hunton & Williams LLP, advising clients on a broad range of privacy and cybersecurity matters, including state, federal, and international privacy and data security requirements as well as the remediation of data security incidents. Adam H. Solomon is an associate at the firm, focusing his practice on privacy and cybersecurity law. Resident in the firm's New York office, the authors may be contacted at asimpson@hunton.com and asolomon@hunton.com, respectively.

Faced with the seeming inevitability of cyber attacks and potentially massive liability that ensues, companies and management are increasingly judged by how well they have prepared for and responded to these types of events. When purchasing, merging with or investing in a company, conducting due diligence of the target company's information assets has become a critical step in protecting investments, limiting liability and mitigating operational, financial and reputational risk arising from the target company's privacy and information security practices.

THE CYBER AND PRIVACY DUE DILIGENCE PROCESS

To manage these risks and liabilities, companies must be proactive. Even if the target company makes representations that it has never suffered a breach, it is undoubtedly only a matter of time before a cyber attacker exploits potential vulnerabilities or a third party identifies ongoing misuse of company information. Moreover, an attack may already be underway. In 2014, an Israeli security firm discovered an ongoing hacking operation targeting banks, governments, research labs and critical infrastructure facilities in Europe that began over 12 years before it was discovered.[1] With network intrusions becoming more persistent, the risk of acquiring a company experiencing an ongoing breach (perhaps unknowingly) has increased.

Potential post-closing integration difficulties also up the ante on diligence associated with information assets. Following a merger or acquisition, companies often face difficulties in integrating their information assets, which can lead to cyber intrusions and privacy mishaps. For example, the merging of the networks or databases of different entities may introduce security weaknesses, induce privacy violations or result in coverage gaps in the company's cyber insurance policy, all of which can be managed more effectively if the companies go into the deal with their eyes wide open.

By conducting cybersecurity and privacy due diligence, purchasers can proactively identify incidents and issues that give rise to concerns regarding the adequacy, reasonableness and appropriateness of the target company's privacy and information security practices. In doing so, the purchaser can develop a roadmap for remediating any material gaps post-closing so that it is well-equipped to manage the cybersecurity and privacy risks of its new investment efficiently and appropriately. Due diligence requests for privacy and cybersecurity-related materials can, however, become overly burdensome and inefficient if the right issues are not identified and the wrong questions are asked. Each due diligence approach should be tailored to the deal and companies at issue. The process should begin with a comprehensive privacy and information security due diligence questionnaire that asks specific questions to the target company and should end with an agreement that contains the appropriate

[1] *See* Liat Clark, *Decade-long Cybercrime Ring Hacked European Banks and Labs*, Wired.Co.UK (Sept. 16, 2014), http://www.wired.co.uk/news/archive/2014-09/16/harkonnen-operation.

representations and covenants concerning privacy and security. As described below, this diligence process should account for the following key areas of risk.

Incident History

There are an assortment of actors threatening corporate information assets today, including cyber criminals, hacktivist organizations and nation states. These threat actors routinely infiltrate corporate networks to steal proprietary information, including customer and employee personal data, payment card information, sensitive financial and strategic information, trade secrets and intellectual property. These parties are not acting alone. To the contrary, they are supported by a sophisticated supply chain of vendors, including software developers, infrastructure providers and money launderers. While some of these attacks are targeted and bespoke, many are carried out using toolkits purchased on the black market that enable non-technical actors to hack corporate networks on a scalable basis using sophisticated malware and other automated methods. As a result of the commodification of hacking, the frequency and volume of cyber attacks has increased.

With the rise in cyber attacks, there is a growing risk of a data breach going undetected or undisclosed prior to closing a deal. Cyber attacks have impacted several deals in recent years. For example, Australian telecommunications provider Telstra reported that it recently became aware of a customer data breach at a subsidiary acquired in the Asia-Pacific region just weeks after closing a $697 million deal to purchase the company in April 2015.[2] Nearly 10 months after acquiring a data broker subsidiary in 2012, Experian was reportedly notified by the U.S. Secret Service that its new subsidiary was being exploited by identity thieves to steal the personal information of allegedly over 200 million individuals.[3] The incident resulted in congressional and regulatory inquiries, a consumer class action brought against Experian, and Experian suing the former owner of its subsidiary for breach of warranty and contract, express contractual indemnification and various tort claims arising from its acquisition. Similarly, in the midst of BNY Mellon acquiring the asset management subsidiary of MBIA in October 2014, a data researcher reportedly discovered sensitive information of the subsidiary exposed on the Internet, including customer account numbers, balances and account access credentials.[4]

---

[2] Mike Burgess, *Pacnet Security Breach*, Telstra Exchange (May 20, 2015), http://exchange.telstra.com.au/2015/05/20/pacnet-security-breach/.

[3] Gerry Tschopp, *The Facts on Court Ventures and Experian*, Experian News Blog (Mar. 30, 2014), http://www.experian.com/blogs/news/2014/03/30/court-ventures/; Jim Finkle & Karen Freifeld, *Exclusive: U.S. States Probing Security Breach at Experian*, Reuters, http://www.reuters.com/article/2014/04/03/us-experian-databreach-idUSBREA321SL20140403.

[4] Edward Krudy & Hilary Russ, *Update 1: Data Breach at Bond Insurer MBIA May Affect Thousands of Local U.S. Governments*, Reuters (Oct. 7, 2014), http://www.reuters.com/article/2014/10/08/mbia-cybersecurity-idUSL2N0S22LB20141008.

To help evaluate the target company's cybersecurity posture and obtain appropriate representations and warranties, the purchaser should investigate the target company's history of cybersecurity incidents, including those related to the company's network, service providers, Web sites, and customers. The clear objective of this inquiry should be to uncover circumstances in which the target company has discovered or been notified of an actual or suspected information security incident, and receive appropriate representations regarding how the company responded to the matter, assessed and satisfied its applicable legal obligations, and remediated the incident. To gain a complete picture of the target company's history of privacy and security incidents, the review also should ascertain the process by which the company monitors, detects, investigates and responds to information security incidents. A lack of appropriate incident response mechanisms increases the likelihood that a breach has gone undetected or undisclosed to management.

Regulatory Compliance

Legal compliance is another key risk to evaluate during the due diligence process. The obligation to comply with privacy and information security laws and standards can raise the integration costs of the acquisition. To remediate deficiencies, the purchaser may need to incur expenses such as updating or replacing computer systems, hiring additional staff, purchasing new services and retaining outside experts to provide assessments. While all companies have compliance challenges, the risk of noncompliance with applicable legal requirements is especially prevalent with startups and midsize companies, which often have less robust, formal and well-funded compliance, legal and information security programs. This can lead to the existence of gaps between such a target's privacy and information security practices and its legal obligations. In these cases, the cost of noncompliance can be significant.

In addition to incurring potentially substantial expenses to remediate privacy and information security issues and align the target company's practices with the purchaser's policies, a regulatory violation could result in fines or civil penalties and extensive settlement agreements that impose onerous information security and privacy requirements on not only the target company but also the purchasing entity. As a historical matter, Federal Trade Commission ("FTC") settlements in the information security arena have been broad, typically enjoining future misconduct and imposing continuing obligations related to the company's information security practices, including third-party audits, for over 20 years. Given how privacy and information security issues were regulated just five years ago, 20 years is a virtual eternity in the data space.

There are many sources of privacy and information laws in the United States and abroad. In the U.S., information privacy and security laws constitute a complex mélange of sectoral-based state and federal laws. Depending on the nature of the target's business, a variety of federal and state laws concerning privacy and information security could apply to the target company's information, including laws regulating

healthcare entities, telecommunications providers, utilities and financial institutions. The FTC has been the primary regulator overseeing privacy and information security practices in the U.S. by using its core consumer protection authority to enforce against unfair or deceptive practices of unregulated entities such as retailers. Industry standards also may impose privacy and security requirements on the target company. Most notably, to the extent the target company receives or processes payment card information, it will have contractual obligations to comply with the comprehensive security requirements of the Payment Card Industry Data Security Standard.

Given the variety of legal mandates applicable to privacy and information security issues, the due diligence process must include an evaluation of the applicable requirements set forth in federal, state and foreign laws, regulatory enforcement actions, and important industry standards concerning privacy, information security and data protection. Based on the applicable requirements, the review should in turn identify and assess areas in which the target's privacy and information security practices fall short of its legal obligations. The target company's privacy and information security policies and procedures serve as key sources of information for conducting such an assessment. To gain a further understanding of the company's privacy and security posture, the compliance review also should evaluate reports prepared by or on behalf of the target company documenting the findings and recommendations from prior risk assessments, privacy and security assessments, or audits or evaluations, including any associated corrective action plans related to those reports. Through these materials, the purchaser can identify red flags and compliance gaps such as out-of-date policies and procedures, inaccurate descriptions of the target's practices or lack of legal compliance, all of which can create significant issues post-closing.

Privacy Representations

To the extent the target company makes privacy representations to its customers, for example, through an online privacy notice or Health Insurance Portability and Accountability Act ("HIPAA") privacy notice, the due diligence review should assess the target's privacy practices and policies representing the way in which it may collect, retain, use, share and process the personal information of consumers. The representations in the target's privacy notices will place limits on the purchaser's ability to use and share this information after the acquisition. Notably, the FTC has issued guidance and sent letters to companies engaging in acquisitions, most recently a letter to Facebook prior to its acquisition of WhatsApp in 2014,[5] regarding its expectation that following a merger or acquisition, the purchaser must honor the prior promises made to consumers by the purchased entity regarding how it may use or share consumer information, or otherwise get express permission from consumers to

[5] Letter from Jessica Rich, Director, Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, Inc. and Ann Hoge, General Counsel, WhatsApp Inc. (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

materially change how their previously collected information will be collected, used or shared after the corporate transaction.[6] For many companies this would be a gargantuan and entirely impractical exercise that should only be taken on with full knowledge of the possibility before closing. The acquisition or merger also might require the company to provide consumers with notice of any change to how it plans to use information collected after the transaction and a choice whether to agree to such changes.

Contractual Liability

The due diligence process also should include an assessment of the target company's contractual relationships with vendors, customers and business partners. Besides assessing the company's risk and legal posture, this review will help identify the next steps for managing the company's vendor and customer relationships after closing in cases where existing contractual language could be enhanced or revised, or ongoing monitoring may be appropriate.

With respect to the target company's vendors, the purchaser should identify third-party privacy and security risks associated with the target outsourcing IT functions to data centers, software developers and other types of service providers. The focus of this review should be on the agreements in place with vendors that host, maintain, receive or transmit the target company's sensitive information. It also is important to ascertain how the target selects, reviews and monitors its vendors. If the target does not take reasonable measures to retain appropriate vendors, include strong contractual protections in its agreements with vendors and monitor its vendors' compliance, then the possibility of a data breach at one of those vendors, known or unknown, increases. Issues commonly found in vendor contracts include agreements with insufficient contractual specifications, broad sharing and usage rights related to the target's information, or a lack of privacy, confidentiality and information security obligations altogether. The review also may uncover that the agreements do not adequately comply with applicable laws, such as when the vendor constitutes a business associate under HIPAA, which requires specific contractual obligations in the business associate agreement.

In addition to vendor agreements, in most cases it will be necessary to evaluate the target company's customer and business partner agreements. These agreements may include additional privacy and information security obligations over and above the target's legal obligations. If such agreements contain terms that establish additional privacy requirements and security specifications such as adherence to information security standards, limitations on data de-identification or restrictions on outsourcing,

[6] *See e.g.*, Jamie Hine, *Mergers and Privacy Promises*, Fed. Trade Comm'n (Mar. 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.

the company may have additional compliance-related challenges and costs associated with meeting such obligations.

Furthermore, in this day and age it is necessary to assess the target's cyber insurance coverage as part of this contractual review. This assessment should analyze both companies' insurance portfolio, including current policies covering cybersecurity, directors and officers, errors and omissions, fidelity and crime, and general commercial liability, to assess potential coverage in the event of a cyber incident and the ramifications the corporate transaction may have on the coverage.

CONCLUSION

Given the pace of technological change we have seen in the recent past and the potential for scalable privacy and information security abuses, the cyber-stakes are at an all-time high. Businesses making investments in data-intensive targets overlook diligence in these key areas at their own peril. Those who take appropriate precautionary measures to assess the privacy and cybersecurity implications of their investments will continue to fare far better than those that fail to do so. By performing due diligence of the target company's privacy and information security practices, businesses will identify key risks to their investment and gain critical knowledge of how potential liabilities may impact their investment.

NOTES

11

Jody Westby, *Cyber Crime Wave: Cyber Insurance Premium Growth Follows the Growing Wave of Cyber Crime*, Leader's Edge Magazine, May 2017

First published in Leader's Edge Magazine: https://leadersedgemagazine.com/articles/2017/05/cyber-crime-wave/

Cyber Crime Wave

CYBER INSURANCE PREMIUM GROWTH FOLLOWS THE GROWING WAVE OF CYBER CRIME.

BY Jody Westby (https://leadersedgemagazine.com/about/contributors/jody-westby) | MAY '17

Cyber insurance is one of the fastest growing insurance markets; it is expected to grow from $2 billion today to $20+ billion over the next decade. It has given agents and brokers the boost they have needed as global insurance rates have steadily declined over 15 consecutive quarters.

In its *Global Insurance Market Index Q4 2016* report, Marsh attributed the decline to "a global market with substantial capacity and an absence of significant catastrophe losses."

Cyber insurance rates, on the other hand, have had positive growth for 10 consecutive quarters, although Marsh data show premiums are now increasing at a slower pace than in 2015, when they rose between 16.9% and 20% throughout the year. In 2016, rates rose by 12% in the first quarter and only 1.4% in the fourth.

This does not necessarily mean the cyber insurance market is stabilizing. It just means the next big attack hasn't happened yet. Just as property-casualty rates are linked to natural disasters and large-scale accidents or events, cyber

insurance rates are linked to cyber crime. The nature of the crime—the industry sector hit, the number of people affected, and the amount of press given to a cyber event—can significantly affect rates.

Reuters reported the 2013 Target Stores and 2014 Home Depot breaches cost the companies $264 million and $232 million, respectively. But the breaches also cost other retailers. Marsh data show a 32% increase in cyber insurance premiums for the retail sector in the first half of 2015. Beazley reported some health insurers who suffered attacks faced a three-fold premium increase.

The insurance market's cyber underwriting process has continued to evolve and mature as lessons are learned from attacks and losses. Insurers are building repositories of claims data to bolster their analysis in the underwriting process. They are also beginning to understand the importance of cyber-security programs that align with best practices. These programs link IT operations, compliance requirements, policies and procedures, technologies deployed, response plans and governance to create a stronger security posture that is better able to withstand cyber attacks.

In the end, however, the insurance market and buyers are still reacting to criminal behavior and the harm caused through cyber crimes, particularly those events that may aggregate exposures. The sophistication of today's attacks is unparalleled, and they are being conducted by a range of actors—teenagers seeking a thrill, lone hackers, insiders, organized crime, terrorists and nation states—each with different motives and end-game strategies. Therefore, it is wise to factor in the unpredictable—the "unknown unknowns"—when determining capacity and pricing parameters. Breaches of personal, health and financial data will continue, but the trend is toward complex, multipronged attacks that may perform several actions (steal data, erase or corrupt data, disclose confidential information, etc.) and attacks with an easy monetary reward.

The increase of ransomware, which is malware that very quickly encrypts all data on a system—as well as online backup files—is alarming. Most companies are not prepared to deal with these attacks (hint: get a bitcoin account now). A 2016 IBM study found that ransomware increased 6,000% in 2016 and is headed toward becoming a $1 billion business.

The Internet of things is all about connecting smart devices, sensors, surveillance cameras, thermostats, etc. to a network and the Internet. It is poised to become a favored means of conducting cyber attacks, which can cause massive network disruptions and business interruption losses.

A recent AT&T report says IoT attacks increased 400% in 2016. No one is prepared to deal with them; not governments, companies, educational institutions, hospitals, underwriters, brokers or agents. I predict by 2018, IoT attacks will become the most serious cyber threat on the planet.

Quite simply, cyber crime will continue to drive purchases of cyber coverage, and it will force changes in insurance products. Large attacks, such as those that hit Target, Sony, Home Depot and Anthem, raised awareness at the board and executive levels and resulted in increased cyber coverage purchases.

A 2016 Zurich-Advisen survey reported 85% of senior executives consider cyber a significant risk, and the Financial Roundtable's 2015 survey (full disclosure: I wrote the report) on board and executive governance of cyber security revealed 63% of boards are actively addressing and governing computer and information security.

That level of awareness drives sales. Marsh had a 25% increase in cyber insurance sales from 2015 to 2016, and Lloyd's of London's CEO, Inga Beale, reported a 50% rise in 2016. The Council's October 2016 Cyber Insurance Market Watch Survey found retail, healthcare and financial services clients were most likely to purchase cyber insurance.

Marsh noted the healthcare, communications, media and technology sectors

led the way.

Cyber insurance sales to small and midsize businesses are also likely to rise. These companies generally have not focused on cyber threats, but they are now increasingly targeted. A 2016 Advisen report says these businesses are often vulnerable and the impact on their operations can be substantial.

All of this means:

- The criminals will keep attacking in more ingenious ways.
- The cyber insurance market is a long way from stabilizing, and insurance companies will struggle for some time to figure out rates and underwriting.
- Clients will remain confused about what cyber insurance they need and how much to buy and will have to engage in risk assessments to help them identify their vulnerabilities and the types of attacks that could have a material impact on their operations or bottom line.
- Brokers and agents will have to do a better job of explaining policies and the types of events that are covered. They will need to understand the threat environment and how attacks can affect clients.
- Legislators will respond to attacks by continuing to pass laws and regulations, such as the EU's General Data Protection Regulation. It goes into effect in May 2018 and requires security measures and imposes stiff penalties for non-compliance. It also forces companies to examine insurance options as a means of transferring risk.

"Regardless of sector, the role of the insurance industry goes far beyond simply providing a cyber policy," says Beale. "It spans the full life cycle—from initial risk assessments to helping build more resilient systems and infrastructure and ultimately to providing the support if and when things go wrong."

Westby is CEO of Global Cyber Risk. westby@globalcyberrisk.com

NOTES

NOTES

12

Jody Westby, *Inside Job: Consider the Range of Attacks Committed by Employees or Trusted Insiders*, Leader's Edge Magazine, June 2017

First published in Leader's Edge Magazine: https://leadersedgemagazine.com/articles/2017/06/inside-job/

Reprinted with permission.

Inside Job

CONSIDER THE RANGE OF ATTACKS COMMITTED BY EMPLOYEES OR TRUSTED INSIDERS.

BY Jody Westby (https://leadersedgemagazine.com/about/contributors/jody-westby) | JUNE '17

When thinking about cyber risks, most companies envision external bad actors trying to hack into their systems or disrupt their operations. They're half right.

Carnegie Mellon University's Computer Emergency Response Team found nearly half (47%) of the respondents to its *2016 Annual State of Cybercrime* survey reported an insider breach, and insiders were responsible for 50% of the breaches of private or sensitive information.

Brokers and agents need to be aware of the types of crimes committed by insiders and understand the differences in coverage. "It is important to determine when cyber is not cyber," says Chris Giovino, Aon's managing director of forensic analysis and crime claims. "Not all cyber acts are covered by cyber insurance. For example, collusion by an insider with an external cyber criminal would most likely be covered under a crime or fidelity policy, not wholly under cyber insurance."

The Sony hack, which resulted in the theft of movies, emails and sensitive internal communications and zeroed out large amounts of data on Sony's servers, was initially blamed on North Korea. Subsequent reports by security experts claimed the attack was perpetrated with insider assistance.

Employers, agents and brokers should consider the range of attacks that might be committed by employees or trusted insiders, such as contractors or business partners with system access. For example, the theft of confidential information, such as pricing and sales data, can lead to the loss of market share if the information should fall into the hands of a competitor who leverages it in the marketplace or if the disclosure results in damage to a company's reputation. This information often is used by a highly mobile workforce and stored on laptops, where it is easily accessible to sales and account personnel. The theft of this sort of data might result from a lost or stolen laptop, or an insider might sell data to a willing buyer.

The theft of highly valuable proprietary data by an insider is usually easier to detect, since these assets are commonly stored in designated repositories with restricted access and user logs. Nevertheless, insiders often commit serious economic espionage. Google's spinoff company Waymo, which specializes in self-driving vehicles, has been in the headlines recently over public allegations that one of its top engineers downloaded 14,000 proprietary files and trade secrets and took them with him to his new position at Uber. Waymo has sued Uber for violations of the federal Defense of Trade Secrets Act and the California Uniform

Trade Secrets Act and infringement of patent rights.

One is reminded in this context of Edward Snowden, the federal contractor who downloaded millions of files from the National Security Agency without being detected. Without good log analysis, monitoring and strict access controls, employees can do the same within any company.

Other highly valued types of data that are susceptible to insider theft, misuse or unauthorized disclosure include employee information, health and benefits data, transactional information, strategic plans and customer data. These data have a strong market value and are easily traded in underground markets.

Compared to external cyber attacks, breaches involving insiders can have a higher financial impact. In fact, 30% of the Carnegie Mellon survey respondents said cyber breaches caused by insiders were more costly than external attacks.

Customer data held in company systems also can put a company in the bull's eye for attack. Manufacturing companies that offer products and services to critical infrastructure industries may have plans of customer facilities, custom specifications, and critical data related to the operation of industrial control systems stored in their computer systems. Often, these data are not encrypted, and the company may not be aware of how much or what types of data it has on its servers or employee laptops. Rather than target multiple critical infrastructure organizations, terrorists and nation-states desiring this information may seek out a vulnerable employee who is willing to obtain it for them.

Not all insider cyber events are nefariously motivated. Insiders also make mistakes or unintentionally cause a cyber incident. For example, companies commonly allow employees to use their own devices, such as laptops, iPads, smart phones and USB thumb drives for business purposes. The use of these devices, however, increases the risk that the device will infect the corporate system with malware. Certain types of applications installed on personal devices, such as peer-to-peer software, could enable unauthorized access to company data. Employees might fall prey to social engineering or fraud tactics and be tricked into emailing personally identifiable information, such as employee W-2 files, to criminals. Again, what many might perceive as a cyber crime may actually be deemed computer fraud by insurance carriers.

An employee's loss of a laptop, CD, thumb drive or smart phone containing personally identifiable information may require a forensic investigation and trigger breach notification laws. This type of loss is covered by most cyber policies. If the employee intentionally provided the data to a third party, however, that could fall under a crime or fidelity policy.

Aon's Giovino offers a tip from experience: "One of the most important steps any company can take when dealing with a cyber event is to have an internal triage of potential events," Giovino says, "and then work with the broker to place all insurance carriers on notice: cyber, fidelity, crime, property and business interruption."

Cyber events, particularly those involving insiders, often unfold in unexpected ways. For example, it is not uncommon for companies to be so disabled from a cyber intrusion that it requires the shutdown of operations to enable a full forensic investigation and system cleanup to be performed. This might trigger cyber and business interruption coverage, as well as property claims.

Brokers and agents face a continuing challenge to stay abreast of the current threat environment and understand the types of insider threats their clients might face. This requires understanding clients' operations and learning about their cyber security program, including policies and procedures, security controls, use of encryption, restrictions on the use of removable media and personal devices, and logging and monitoring. Companies that think through the insider threat and mitigate these risks through a strong security posture and well-considered coverage will have the best cyber risk management strategies.

Jody Westby is CEO of Global Cyber Risk. westby@globalcyberrisk.com

NOTES

NOTES

13

Jody Westby, *Starving Your IT Budget: Your Failure to Upgrade Means Your Luck May Be Over*, Leader's Edge Magazine, July/August 2017

First published in Leader's Edge Magazine: https://leadersedgemagazine.com/articles/2017/07/starving-your-it-budget/

Starving Your IT Budget

YOUR FAILURE TO UPGRADE MEANS YOUR LUCK MAY BE OVER.

BY Jody Westby (https://leadersedgemagazine.com/about/contributors/jody-westby) | JUL/AUG '17

The recent WannaCry ransomware outbreak was the major global cyber attack that security experts have been warning of for years. It wreaked havoc by encrypting data on an estimated 230,000 computers in 150 countries and demanding a $300 ransom paid in bitcoins to get the computer decrypted (which reportedly did not work in some cases).

If the ransom was not paid within three days, the amount doubled. Payments made to the bitcoin wallets used by the hackers indicate higher amounts, most likely to decrypt more than one computer. @actual_ransom—a Twitter bot that is watching the bitcoin wallets associated with WannaCry—indicates that, at the time of writing, about 337 payments had been made, equaling $134,859.54.

Britain's National Health Service was crippled, canceling surgeries, chemotherapy and other medical necessities. Other major organizations hit included Federal Express, Spain's Telefonica and Deutsche Bahn.

The malware uses a vulnerability in Windows' operating systems that the National Security Agency (NSA) discovered more than five years ago. According to *The Washington Post*, the vulnerability was so serious the NSA recognized it could cause widespread harm if leaked. The NSA discussed

internally whether to notify Microsoft so it could develop a patch for the vulnerability but decided against it to exploit the vulnerability for intelligence gathering purposes.

The malware was revealed in August when a hacking group called The Shadow Brokers disclosed an entire archive of NSA cyber offensive tools it had stolen. The NSA finally notified Microsoft, and a patch was issued in March. But the patch was made available for only those Microsoft operating systems that are “in support,” meaning those maintained by Microsoft with patches or upgrades issued to licensed users.

When the WannaCry ransomware hit on May 12, 2017, companies had only had two months to apply the patch to their systems. Patches are easier for individuals to apply than companies and governments, which have to test the impact on applications and systems before deploying patches in a production environment. It takes time, and at the end of two months, many companies had not yet deployed the patch on all of their systems.

Despite the severity of the vulnerability, Microsoft did not issue a patch for its Windows systems and servers that are still in use but “out of support,” such as the Windows XP operating system and Windows 2003 servers. According to recent reports, Windows XP is still running on millions of computers and is the third most popular operating system. An estimated 18% of organizations are using Windows 2003 servers in their IT environments. Around midnight the day of the attack, Microsoft finally issued a free patch for XP systems (Microsoft usually charges $1,000 per computer for an XP patch) and 2003 servers.

Now, more trouble has been set loose. Shortly after the WannaCry attack, a new variant of the malware, called EternalRocks, was released that contains six additional NSA exploits and targets Windows machines.

EternalRocks may be more dangerous than WannaCry. Researchers have determined that it installs a private networking software on the computer called TOR, which conceals Internet activity. TOR is used by the malware to respond

to the controller of the malware and begin downloading and self-replicating on the infected computer. The danger is that EternalRocks currently appears to be in stealth mode and just infecting computers; what is unknown is what it will do when activated. It could exfiltrate data via TOR or take other malicious actions, such as corrupting or zeroing data.

Starving IT

So what does this have to do with IT budgets? Everything. Many organizations are not funded to:

- Fully staff a dedicated information security team
- Develop an enterprise security program consistent with best practices and standards (including robust incident response and business continuity and disaster recovery [BC/DR] plans)
- Keep software and hardware patched and within vendor support
- Replace old legacy applications that require out-of-support operating systems.

Almost every client we work with struggles to get enough money to implement and maintain a robust cyber-security program, and it doesn't matter if they have revenues in the billions or low millions. The security teams are often small, consisting of only a few people, some whom are IT personnel with added responsibilities for cyber security. Many do not have security job descriptions or hold cyber-security certifications or degrees. They learn as they go, and their companies might not pay for training, certifications or fees to attend cyber-security conferences.

Organizations commonly have Windows XP and/or Windows 2003 servers in their production environments. Sometimes this is because old legacy applications (that businesses refuse to replace) often require the XP operating system, and other times it is because IT and security have not been given the budget they need to replace out-of-support equipment. So security teams hobble along as best they can, juggling priorities and trying to keep attackers at bay.

The lack of adequate IT and cyber-security funding also frequently results in poorly developed incident response and BC/DR plans. These two areas usually have the lowest scores in our cyber-risk assessments. This means companies are likely to have a chaotic incident response when a serious incident occurs and may not be able to fully restore data if erased, corrupted or encrypted.

Cyber-security professionals, by and large, are dedicated and want to build a strong cyber-security program. But executives must understand malware can readily find out-of-support equipment or software and exploit it.

All of these factors converge to create a global network of organizations with legacy apps, out-of-support equipment and systems, insufficient cyber-security expertise, and weak to mediocre security programs with gaps and deficiencies that help enable these attacks. The WannaCry malware just encrypted data; these other NSA exploits can leave the infected computer open to remote commands so it may be “weaponized” on demand or exfiltrate data.

We hear a lot about what needs to be done to curb cyber attacks: better information sharing, more government leadership and funding, improved assistance from law enforcement, and new laws and regulations. But we do not hear enough about organizations starving IT budgets to the point they contribute to the problem.

Agents, brokers and their clients are equally at risk of attack, and the first and best line of defense is a robust budget line for IT and cyber security. From my side, we need to do a better job of educating organizations on the costs associated with cyber attacks so they can be weighed against IT and cyber-security budget requests.

A complex forensic investigation can cost several million dollars, including business interruption costs, equipment replacement costs, remediation consulting costs, and regulatory and legal costs. That doesn’t even include potential reputation and brand damage.

In the end, the organization still had to upgrade equipment, address gaps and deficiencies, and improve its security posture—it just cost more. A dollar in time can stop cyber crime.

Westby is CEO of Global Cyber Risk. westby@globalcyberrisk.com

NOTES

14

Jody Westby, *Spreading Cyber Around: Cyber Coverage Is Popping Up in Multiple Places. Look Widely to Recover Claims*, Leader's Edge Magazine, October 2017

First published in Leader's Edge Magazine: https://leadersedgemagazine.com/articles/2017/10/spreading-cyber-around/

Spreading Cyber Around

CYBER COVERAGE IS POPPING UP IN MULTIPLE PLACES. LOOK WIDELY TO RECOVER CLAIMS.

BY Jody Westby (https://leadersedgemagazine.com/about/contributors/jody-westby) | OCTOBER '17

Cyber attacks are becoming increasingly complex, lengthening recovery times and taking a greater toll on business operations. Numerous attacks have zeroed out servers; corrupted, encrypted or exfiltrated data; or caused sustained denial of service to systems. Many of these consequences may occur in a single attack, and coverage under a cyber policy may not be the only avenue to recover losses.

Cyber insurance is a growing market, but it's not the only place to look for coverage from a cyber attack. Robert Parisi, managing director for Marsh's FinPro practice, says, "As losses get larger, people are examining their coverage and often taking a shotgun approach to claims and notifying everyone they can if they don't have express cyber coverage." Parisi says, "The best approach is not to view a cyber event in isolation but to look at all policies—property, E&O, general liability, terrorism, kidnap and ransom, and fidelity—and see where aspects of a cyber event may be covered."

Cyber Claim History

In the early days of cyber attacks, companies made claims under their property and commercial general liability policies. Coverage questions initially revolved around whether the loss of data could constitute a direct physical loss or damage under a property policy.

One of the first property policy disputes, *Home Indemnity Co. v. Hyplains Beef,* was based on a claim for business interruption losses arising from a disrupted computer system. In 1995, the federal district court dodged the question of whether the loss of data was a direct physical loss and focused on actual language of the business income section of the policy. The policy required a "suspension of operations." The trial court denied the claim because, although the disruption made the computer system less efficient, the "suspension" of plant operations had not occurred. The Tenth Circuit affirmed.

However, a case in 2000, *American Guarantee & Liability Insurance Company v. Ingram Micro,* did find that the loss of data constituted physical damage under the company's business interruption policy. The court noted, "Lawmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is damage; and when a computer's software or network is altered, there is damage."

The insurance industry scrambled to clarify the issue by specifically excluding electronic data from property coverage. Indeed, the current Insurance Services Office's Building and Personal Property Coverage Form excludes "The cost to research, replace or restore the information on valuable papers and records, including those which exist on electronic or magnetic media, except as provided in the Coverage Extensions." The current form's coverage extensions provision limits recovery to $1,000 at each location.

Bucking the Trend

Some insurance companies, however, are turning away from the ISO language and pursuing the cyber insurance market by including cyber coverage in property policies. FM Global, Affiliated, Liberty, AIG and Zurich all include elements of cyber coverage in their company-issued property policy, while XL Catlin and Allianz have cyber extension endorsements available. FM Global's website states that its Global Advantage policy covers:

- Damage to data, programs or software created by harmful viruses or other malware
- Computer network service interruption due to malicious cyber activity
- Third-party data services interruption (cloud outage) leading to business interruption and/or property damage
- Resulting property damage and business interruption on an all-risk basis.

This type of property coverage can be particularly important when malware infestations require expensive and time-consuming eradication measures, which may involve replacing equipment.

John Dempsey, founder of Terrabella Risk Consultants, says that as attacks increasingly impair system operations, rather than steal data, companies should pay close attention to how an attack impacts the company's computer systems. "Multipronged attacks are driving multiple claims," he says. Dempsey's expertise in quantifying the impact of cyber attacks and supporting business interruption claims has enabled him to understand where other types of coverage may come into play after a cyber event. "If the nature of the IT hardware changes and a client can show loss of functionality, a credible argument can be made that the loss of use of the equipment supports a property claim that the equipment was damaged."

The recent attack of NotPetya malware is a good example. The malware was a combination of powerful malware tools that deeply infiltrated systems to destroy data and take over file systems. NotPetya created massive business interruptions at large corporations such as Maersk, Federal Express, and Reckitt Benckiser. Maersk's CEO has estimated the attack will hit the company's third quarter financial results by $200 million-$300 million. Shipping

company TNT, a subsidiary of FedEx, was still feeling the impact of NotPetya three weeks after the attack, with manual processes still in place and widespread delays in service and invoicing.

Mike Andler, property practice leader at Lockton, has been carefully monitoring the cyber coverage extensions in the property insurance market. “We will have to wait and see the result of recent first-party cyber claim activity and its ultimate effect on the marketplace, especially with respect to terms and conditions, price and available limits.” Referring to that shotgun approach he currently sees, Parisi cautions that insurance companies may begin specifically excluding cyber from those traditional policy products that aren’t necessarily intended to cover cyber events.

Accordingly, organizations have to carefully monitor their cyber coverage. The simple data breaches that required only notification to authorities and victims have given way to complex attacks that require a comprehensive approach to cyber risk management. Today, boards and executives must delve deeper when managing cyber risks and examine the interdependencies between business units and IT operations.

They need to determine:

- What types of cyber attacks are possible
- What the impact on operations would be
- What insurance coverage is needed
- What financial limits are required.

Understanding the potential impact of cyber attacks is a difficult exercise that requires technical, operational, legal and insurance expertise. Brokers and agents can assist by helping clients view cyber risks as enterprise risks and examining all their policies to identify possible coverage areas for cyber claims. They also can help identify experienced forensic, technical and legal resources that can assist clients in the event of an incident and, perhaps most importantly, help manage the post-event claims process.

Westby is CEO of Global Cyber Risk. westby@globalcyberrisk.com

NOTES

15

Jody Westby, *Cybering Up for Your Safety: This 15-Step Program Will Help You Recover from Unsafe Practices*, Leader's Edge Magazine, March 2018

First published in Leader's Edge Magazine: https://leadersedgemagazine.com/articles/2018/03/cybering-up-for-your-safety/

Reprinted with permission.

Cybering Up for Your Safety

THIS 15-STEP PROGRAM WILL HELP YOU RECOVER FROM UNSAFE PRACTICES.

BY Jody Westby (https://leadersedgemagazine.com/about/contributors/jody-westby) | MARCH 2018

After a number of significant cyber attacks last year, many organizations are looking for ways to make 2018 a "cyber secure" year. But coming up with a list of solutions to improve an organization's security posture is no easy task.

An enterprise security program is a complicated mash of hardware, software, networks, configuration settings, and operational policies and procedures. There are numerous best practices and standards, and most have more than a dozen categories and hundreds of requirements encompassing technical, administrative and physical realms.

It is no wonder business leaders often seem uncertain about whether their cyber-security budgets are being spent on projects or technologies that really will make their data and systems more secure. A more simplified view is required.

One way to reduce the complexity is to step back and ask which cyber-security program requirements are *critical* to reducing risk, which are *important* to reducing risk, and which are *basic* requirements in reducing risk.

- **The critical requirements** of a security program are those that are essential in maintaining any semblance of a strong security posture and, if not performed, could result in significant harm to data, systems or the organization.
- **The important requirements** are essential, but if they are not performed or are partially performed, the harm may be less consequential than that flowing from critical requirements.
- **The basic requirements** are security program activities that are best practices but may result in less impact on the organization if they are not performed or are performed poorly.

These are generalizations, of course, but let's consider some examples. Access controls are critical. If an organization does not have sufficient access control policies and procedures and supporting technologies in place, it will not be able to secure its data or systems, hold users accountable, or maintain accurate records for compliance and forensic purposes.

Equipment inventories are important. Companies should maintain an inventory of equipment provided to employees and check off return of equipment upon employee departure. If they do not, there is a risk that a phone or laptop might not be returned and some company data may be on it. This exposure is limited to internal individuals and may be mitigated by other controls, such as encryption and access policies.

Secured telecommunications cabling is a basic requirement. While it is always a best practice to secure telecommunications cabling against interference or damage, on the whole, most companies have little risk of their cabling being tampered with.

Organizations have limited resources for IT and cyber-security programs, and many executives do not fully understand what an enterprise security program really is or know what is required by best practices and standards. (For more on that, read my previous column **"Starving Your IT Budget." (http://leadersedgemagazine.com/articles/2017/07/starving-your-it-budget)**) In the face of an increasingly sophisticated threat environment,

executives struggle with understanding which cyber-security activities will matter the most in defending against cyber attacks and protecting company assets.

As a general rule, if companies make sure they meet the *critical* requirements—and add a few *important* ones—they will have a strong cyber-security foundation on which to build and a decent chance of detecting, deterring and preventing cyber attacks. In a recent review of the 114 requirements for the ISO 27001 standard for information security, my team tagged 58 requirements as critical, 32 as important and 24 as basic.

From the 58 critical requirements, we identified the top 15 that we believe are essential activities for all cyber-security programs. If you undertake these cyber-security solutions, you'll put your organization on stronger footing against cyber attacks in 2018.

When reviewing cyber-security budgets and resource allocations, executives should check to see how much of the funding is for activities on this list of resolutions. Management also now has a solid list of critical requirements they can refer to when discussing priorities with IT and security personnel. Agents and brokers also can use this information to better serve their clients and help them make informed decisions on managing cyber risks and improving their organization's cyber-security posture.

15 Steps to Safer Cyber Security (http://leadersedgemagazine.com/articles/2018/03/15-steps-to-safer-cyber-security)

Westby is CEO of Global Cyber Risk. westby@globalcyberrisk.com

15 Steps to Safer Cyber Security

1. Assign roles and responsibilities for cyber security, both within the executive ranks and at the operational level.
2. Maintain up-to-date inventories of applications, data and hardware—an organization has to know what assets it has in order to secure them.
3. Demand strong access controls; use two-factor authentication for remote access (e.g., password and biometric authentication or fob code).
    a. Do not allow shared user accounts.
    b. Require strong passwords or biometric authentication.
    c. Change all default passwords, even on printers, copiers, scanners and digital cameras.
    d. Limit access to only the data and systems needed for job performance.
    e. Privileged access for system administrator functions should be controlled and monitored. Only system administrators can install software or add hardware.
4. Install anti-malware software, automatically update it and run scans frequently. Use next-generation firewalls.
5. Use only equipment and software that is within vendor support (check Microsoft products by referring to this site: bit.ly/2aS8mHe).
6. Get rid of legacy applications that require out-of-support software or operating systems (no matter how much the business users love them).
7. Update all software and apply patches within one month of notification—sooner if serious vulnerabilities have been identified.
8. Allow local admin rights on workstations or laptops only where absolutely necessary.

9. Use full-disk encryption for laptops and encrypt sensitive data at rest.
10. Use network segmentation to restrict users and applications to defined areas of the network.
11. Develop an incident response plan capable of managing all types of incidents and test it involving all stakeholders.
12. Regularly back up systems and data, store backups offsite, and develop and test recovery plans.
13. Restrict the use of removable media (thumb drives, CDs, external hard drives).
14. Develop and implement cyber-security policies and procedures in alignment with best practices and standards.
15. Perform regular risk assessments of the cyber-security program, including reviews of cyber insurance.

NOTES

NOTES

16

Jody Westby, *Cyber Property: How Much Risk Do You Want to Keep In-House?,* Leader's Edge Magazine, October 2018

First published in Leader's Edge Magazine: https://leadersedgemagazine.com/articles/2018/10/cyber-property/

Cyber Property

HOW MUCH RISK DO YOU WANT TO KEEP IN-HOUSE?

BY Jody Westby (https://leadersedgemagazine.com/about/contributors/jody-westby) | OCTOBER 2018

Not so long ago, as outsourcing, co-location facilities and cloud services began to take hold, risk managers and information security personnel scrambled to manage vendor cyber-security risks.

Everyone was afraid of what could happen to company data or operations in the hands of a third-party provider. Today, however, these vendors seem like a safe haven compared to the risks and costs associated with running an in-house data center and cyber-security program.

Attacks no longer require someone to click on a link or open an attachment. In the past year, large global companies have been hit by malware that exploited out-of-support equipment and unpatched software and crippled operations for weeks. Maersk, Merck and Federal Express were three of the most visible companies hit. Maersk's chairman, Jim Hagemann Snabe, told World Economic Forum leaders that the company had to reinstall its "entire infrastructure," consisting of 4,000 servers, 45,000 workstations and 2,500 applications. Business interruption losses at the companies ranged from $300 million to $670 million each.

In this environment, companies that have been scrimping on IT budgets and stalling on replacing legacy apps are now in the bull's-eye. Why? Because hardware companies continually patch vulnerabilities and update their products and they eventually stop supporting older equipment. Even though the older servers may still run just fine, their known vulnerabilities can be exploited by criminals. Out-of-support software can be just as bad. CFOs know how expensive it can be to move to a new enterprise application, and business units are famous for refusing to give up favored legacy apps. These apps usually run on older versions of operating systems. Thus, companies end up with Windows XP or other out-of-support operating platforms that enable these legacy apps to be operational, but they bring risk to the organization in the process. The WannaCry malware that infected 230,000 computers in more than 150 countries exploited unpatched Windows systems, many of which were out-of-support.

Maintaining a cyber-security program requires a team of personnel with appropriate education, certifications and experience. Some companies have pinched pennies on security staff, and others simply cannot find suitable candidates to hire in this tight job market. Security architects and network engineers play an important in-house role in designing the system architecture and determining configuration settings and security controls that help protect the system and data. Without an adequately staffed team of IT and security personnel, critical activities either do not get completed on time or they are not performed at all. This includes patching of software, particularly non-Windows software, because these patches have to be specially applied outside of the regular Windows "push patch" cycle. Since patches fix vulnerabilities, every instance of unpatched software creates an opportunity for exploitation.

Security programs also require a suite of security tools, which often demand training and expertise to deploy and use them. When security tools are installed but the staff does not know how to use them, the license fees are wasted, and the ability to identify risks or attacks decreases. Logging, incident response, and backup and recovery are also commonly given less than full attention when resources are thin. The consequences can be particularly painful when an

attack hits. Without logs, in many instances it is difficult to conduct an adequate forensic investigation. Tested backup and recovery plans are critical, particularly in attacks of ransomware that encrypt a company's data or malware that zeroes out servers and computers.

Farm It Out

Handing off an organization's hardware, software, network and staffing issues to a vendor is an increasingly attractive option. Major vendors today have sophisticated system architectures, hardware that is within vendor support, strong controls, a full security program, and highly experienced IT and security personnel. In addition, they generally have excellent physical security, good surveillance and monitoring systems, more-than-adequate HVAC systems, back-up generators and resilience in connectivity. Many cloud providers also offer a suite of services and tools to assist with incident response, logging, backup and recovery on the client side.

The trust a company places in a vendor hinges on the vendor's reputation for protecting the client's systems and data. Therefore, these service organizations devote considerable attention to securing their network, applications, data, people and processes. Most vendors have an annual security audit performed in line with standards from the American Institute of CPAs, which produces what is known as a SOC-2 report. According to the AICPA, "These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems."

Companies do not have to farm out all operations to vendors, however, as they may choose to keep their data centers and outsource just the security activities. Many companies that have their own data centers are looking to managed-security service providers to take on some of the load of the security program. These providers are capable of taking over most of the activities of an

enterprise cyber-security program, enabling companies that choose to keep their IT operations to have robust security capabilities performed and maintained by a third party. These services are particularly attractive to small and midsize companies that use technology extensively and need to protect their data and systems but find it financially prohibitive to develop and maintain a strong enterprise security program.

Cloud offerings, such as Microsoft's Office 365 and Azure environments, are enabling companies to free themselves from maintaining a data center. Software as a service (SaaS) and outsourced enterprise application providers are freeing organizations from patching and application maintenance.

Antares Capital—one of my clients—is an example of an organization that chose to move in a futuristic direction (in this case, after it was spun off by GE). Instead of taking legacy apps and aging equipment with it, its chief information officer, Mary Cecola, chose to stand up entirely new IT operations by leveraging the Microsoft Azure and Office 365 environments and utilizing enterprise applications that are SaaS or vendor hosted.

The organization now has all thin clients (monitors and keyboards without hard drives or memory) and a few closets with routers. All other infrastructure and equipment are owned by Microsoft and are in the Azure environment. Antares is able to properly manage operations with a smaller IT and security staff. The security team has established a security operations center that monitors system activity and interfaces with the vendors.

"We are sharing risk with our vendors, saving financial resources and better managing the risk of attack," Cecola notes. "We hired excellent personnel with expertise in cloud and vendor environments and IT and security management and are now able to devote resources to the specific IT and security needs of the business while leaving a lot of the nitty-gritty technical activities and issues to the vendors. We developed an incident response plan and recovery strategy

that dovetails with our vendors and leverages their capabilities. While my peers still struggle with many of the issues of in-house shops, going with the Azure cloud and SaaS providers was probably the best decision of my career."

Agents and brokers will serve their clients well if they help them examine the risks associated with their IT operations and discuss risk-transfer options, including the use of third-party providers.

Westby is CEO of Global Cyber Risk. westby@globalcyberrisk.com

NOTES

17

Jody Westby, *Preparing for New Cyber Threats: What's on the Horizon in 2019? Make Sure You've Got a Comprehensive and Tested Plan*, Leader's Edge Magazine, December 2018

First published in Leader's Edge Magazine: https://leadersedgemagazine.com/articles/2018/12/preparing-for-new-cyber-threats/

Preparing for New Cyber Threats

WHAT'S ON THE HORIZON IN 2019? MAKE SURE YOU'VE GOT A COMPREHENSIVE AND TESTED PLAN.

BY Jody Westby (https://leadersedgemagazine.com/about/contributors/jody-westby) | DECEMBER 2018

As companies look to the year ahead, they should make sure they are prepared for the types of cyber attacks they might encounter in 2019. The cyber threat environment is more sophisticated than ever, and nation-states have increasingly played a role, often in coordination with other actors.

Even the best chief information security officers are evaluating their programs against current threats and beefing up.

Many companies, however, have inadequate cyber-security programs and are not prepared for multipronged attacks or those that could create significant business interruption. For example, in nearly every cyber-risk assessment we conduct, the two lowest-scoring areas are incident response and business continuity/disaster recovery. In addition, many organizations have not identified mission-critical functions, do not have current or adequate inventories of their applications and data, and have not assigned ownership to these assets. When trouble hits, these gaps make for a pretty hot mess.

So it's a two-pronged problem: an organization must first understand its assets and what they are used for and then understand the types of attacks that could hit them. When an organization has not paid attention to its assets, chances are it is clueless about its threat environment, its preparedness to counter an attack, and its ability to keep functioning.

Engage Business Units

Internally, many organizations still tend to view IT and cyber security in a silo and try to be involved as little as possible with them. They just want the systems—and business—to keep running. That attitude ignores the accepted best practice that business units should "own"—and be responsible for—the data and systems they use to perform their business functions. Business owners should approve access to their applications and data and authorize a system to operate, thereby taking responsibility for the risks the system and data bring to an organization. This is how risk management is spread across an organization.

In reality, however, managers somewhere in the organization usually request access to applications or data for new hires and send the request to IT, which then implements access. Business owner approval is not a common practice.

If business owners are not engaged in controlling access to their systems and data, they are likely not very involved in what happens during incident response or disaster recovery. Thus, a major incident sends IT and security teams scrambling to identify critical applications, their dependencies and the business functions that have been affected.

Test Your Plans

Well developed disaster recovery plans, based on an analysis of the impact on business, are an essential element of cyber-security programs, but they must be tested. Consider the company whose IT team confidently told management it did not need to pay a ransom because the company could simply restore the

data—except that the company hadn't tested its plan and ended up losing six months of data. Or consider the companies that thought they had it made in the shade with constant replication from one site to another, enabling them to switch to the alternate site at any moment. Those companies forgot about ransomware, which ran through their systems encrypting all their data—and their replicated site data (because they forgot about needing an offsite backup).

New Threats

Now, consider the new threat environment, which utilizes the treasure trove of NSA cyber tools and zero-day exploits that were released in 2016 by the hacking group Shadow Brokers. Portions of these were used in the severe WannaCry, Petya, and NotPetya attacks in 2017. Projections on 2019 cyber attacks continue to list malware, ransomware, botnets, denial of service, website "drive-by campaigns" (which infect when you visit a website), phishing attacks, and advanced persistent threats (malware that lurks inside your system and stealthily attacks).

The exploitation of internet of things devices has been behind several of the worst cyber attacks in the past couple years, such as Stuxnet (and its offspring), which attacked programmable logic controllers in industrial control systems, and the Mirai botnet and similar bots, which attacked IoT devices and used them to cause huge denial of service attacks, shutting down major websites and turning off heating in buildings.

Expect more IoT attacks in 2019.

An estimated 23 billion IoT devices are connected to the internet now—everything from appliances to thermostats to building monitors and controls—with growth expected to reach 31 billion by 2020. Many of these devices are not patchable, were not built with embedded security, and are not included within the inventories of hardware in many cyber-security programs.

In 2019, we also will see more “clickless” attacks that exploit vulnerabilities in out-of-support hardware and software, such as WannaCry and NotPetya. This type of malware presents a major risk to the many organizations that have hung on to old equipment and applications.

Dmitri Alperovitch, co-founder and CTO of CrowdStrike, investigated and brought to light some of the most serious cyber-espionage attacks. Regarding the current threat environment, he said: “CrowdStrike research indicates that on average it takes an adversary one hour and 58 minutes to break outside of the initial point of intrusion and get deeply embedded into the network. This means that the best organizations should strive to detect intrusions within one minute, investigate within 10 and eject the adversary within the hour to stay ahead of the threats.” That’s a tall order, but it underscores the severity of attacks we are facing in 2019.

When organizations consider their cyber coverage in 2019, they would be well advised to think beyond breaches of personally identifiable information and look under the hood to see if some of the basics in their cyber-security program—such as asset inventories, incident response and business continuity and disaster recovery—are well developed and tested. The threat environment sets the pace, and companies that do not keep up with mature cyber-security programs and test their data recovery capabilities will be the easiest targets and suffer the biggest losses. Brokers and agents will do well to help their clients assess their vulnerabilities and the maturity of their cyber-security programs and develop a coverage plan to match.

Westby is CEO of Global Cyber Risk. westby@globalcyberrisk.com

NOTES

NOTES

18

The Latest Insights from Privacy and Data Security Regulators (June 3, 2019)

Reprinted from the PLI Course Handbook, Nineteenth Annual Institute on Privacy and Data Security Law (Item #219182)

BIOGRAPHICAL INFORMATION

Ruth Hill Bro (Chicago) has focused her legal career on advising businesses on privacy and information management strategy, cybersecurity, global compliance, the electronic workplace, and e-business. She has been featured as a speaker on these issues over 160 times and has over 90 published works on these topics. These works include the first (2013) and second (2018) editions of *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals,* which won the 2018 ACLEA Best Publication Award (contributing author, ABA; ambar.org/cybersecurity); *Data Breach and Encryption Handbook* (two chapters, 2011, ABA); *The E-Business Legal Arsenal: Practitioner Agreements and Checklists* (Editor, 2004, ABA); *Internet in the Workplace: Managing Organizational Access* (designed and taught one-day course throughout the U.S. and co-authored book, 1997, Software Publishers Association); *Online Law* (five chapters, 1996, Addison-Wesley); and her column *CPO Corner: Interviews with Leading Chief Privacy Officers* (2005-present, published in *The SciTech Lawyer* magazine).

Ruth is a longstanding leader in the American Bar Association (ABA), where she co-chairs the ABA Cybersecurity Legal Task Force (ambar.org/cyber), serves on the ABA E-Mail Stakeholder Committee, and is a leader in the ABA Section of Science & Technology Law (SciTech). In SciTech, she is a Senior Advisor for the Privacy, Security, and Emerging Technology Division, a member of the Planning Committee (2015-2019) for the ABA's first four Internet of Things (IoT) National Institutes, and the Section's Liaison to the ABA Commission on Women in the Profession. She also served as SciTech's 2008-2009 Section Chair, Membership and Diversity Committee Chair (2009-2016), and E-Privacy Law Committee Founder and Chair (2000-2005). Ruth likewise served two three-year terms (2009-2015) on the ABA Standing Committee on Technology and Information Systems (the second term as Chair), as a liaison to the ABA Standing Committee on Continuing Legal Education (2012-2015), on the ABA Commission on the Future of Legal Services (2014-2016) (a two-year presidential commission to improve access to, and delivery of, legal services in the U.S.), on the ABA Standing Committee on Disaster Response and Preparedness (2016-2017), and on the ABA Board of Governors Communications Task Force (2017).

Ruth has served on many of the top advisory/editorial boards in the privacy, data security, and technology field (including *The SciTech Lawyer*, *DataGuidance* (U.S. Panel of Experts), *Internet Law & Strategy, The Privacy & Data Protection Legal Reporter* (Executive Editor/Chairman of

the Board of Editors), and BNA's *Privacy & Security Law Report*) in addition to the boards of two arts organizations and the Illinois Institute for Continuing Legal Education. She has been recognized as a leader by numerous organizations, including for four consecutive years in Ethisphere Institute's annual list of Attorneys Who Matter (data privacy/security). Her views have been noted by the *Wall Street Journal, International Herald Tribune, New York Times, Economist Intelligence Unit, ABA Journal, National Law Journal, Corporate Counsel, BNA Privacy & Security Law Report, CyberInsecurity News, FCW/Federal Computer Week, Legaltech News, Bloomberg Radio,* and *CNBC.*

Ruth started her legal career at McBride Baker & Coles (now Holland & Knight) and then spent nearly a decade at Baker & McKenzie, where she was a partner in the Chicago office and founding North American member of the firm's Global Privacy Steering Committee. Before getting her J.D. from the University of Chicago, Ruth had a successful career in major gifts fundraising at Northwestern University, where she earned her B.A. in English and Political Science. She won first place in *New York Law Journal's* fiction contest for her short story, *Privilege,* and before that second place in *Chicago Lawyer's* fiction contest for her short story, *Her Father's Daughter.*

Contact: (630) 926-1273; ruth.hill.bro@gmail.com

Table of Contents

- "Get SMART on Data Protection: Training and How to Create a Culture of Awareness," by Ruth Hill Bro and Jill D. Rhodes, Chapter 13, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals,* ABA Cybersecurity Legal Task Force (2d ed. 2018), ambar.org/cybersecurity
- "Lawyers' Legal Obligations to Provide Data Security," by Thomas J. Smedinghoff and Ruth Hill Bro, Chapter 4, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals,* ABA Cybersecurity Legal Task Force (2d ed. 2018), ambar.org/cybersecurity.
- For cybersecurity/data protection information, see the website of the ABA Cybersecurity Legal Task Force (co-chaired by Ruth Hill Bro), which focuses and coordinates the ABA's cybersecurity legal and policy analyses/assessments and identifies, compiles, and creates cybersecurity resources from a cross-disciplinary perspective, at www.ambar.org/cyber.

Chapter 13

Get SMART on Data Protection Training and How to Create a Culture of Awareness

Ruth Hill Bro and Jill D. Rhodes

I. Data Protection Training Basics and Core Principles

Any business that works with personal and sensitive data must develop a strategy for protecting that data. When assessing how to do so, organizations, including law firms, often mistakenly rely on technology as the solution. In fact, four factors are key to implementing a proper information security and data protection program in any setting:

- Establishing the appropriate *governance* for the data, such as policies and the oversight of an executive level committee tasked with reducing data protection risk;
- Ensuring that the *people* working with the data know how best to protect it;
- Assessing data protection and usage *processes*; and
- Employing appropriate *technology* to protect the network.

These four factors work together to develop an overarching and effective program.

This chapter focuses on the people aspect of that equation, but other factors (e.g., governance and processes) also come into play. Most data missteps in law firms and other businesses are directly linked to something an employee or contractor did, whether intentionally or unintentionally. The easiest way to address this risk is to educate employees and others about the risk and their role in protecting personal and sensitive data.

Education and training can be provided by many facets of the organization, whether human resources (HR), the chief privacy officer (CPO), the chief information security officer (CISO), or others. Regardless of which groups do the training, it is critical that they work together to produce a common vision and message that is then disseminated across the organization.

A. Why Train on Data Protection?

All organizations, including law firms, are increasingly recognizing that data underpins virtually everything that they do and—like other valuable business assets—should be protected.

The trend is to adopt a reasoned and comprehensive strategy that makes data protection a part of the corporate culture and the job of every individual working for the business (partners, associates, paralegals, interns/law students, information technology (IT), HR, executives, administrators, administrative assistants, and other staff).[1] Such an approach is designed to:

- Minimize missteps that can hit the bottom line (costly litigation; time and resources consumed in responding to government, press, or attorney disciplinary commission inquiries or investigations; adverse media coverage; damage to client or customer relationships; and so on), and
- Help businesses achieve a competitive advantage, enhance their profile and image, and enrich their relationship with clients and customers.

1. This trend is in keeping with the "Privacy by Design" (PbD) and "Security by Design" (SbD) movements that are transforming the way that businesses protect data in an information-driven age. *See, e.g., Privacy by Design: The 7 Foundational Principles,* by Ann Cavoukian, Ph.D., Distinguished Expert-in-Residence, Privacy by Design Centre of Excellence, Ryerson University and former Ontario Privacy Commissioner, at http://www.ryerson.ca/pbdce; *see also* Fed. Trade Comm'n, *Start with Security: A Guide for Business,* http://www.ftc.gov/startwithsecurity for insights and guidance on SbD gleaned from over 50 FTC data security settlements.

Yet making data protection a part of the corporate culture is easier said than done:

- Properly addressing data protection issues can require a comprehensive understanding of rapidly changing applicable law in 50 states and territories, at the federal level, and globally (where client or customer data might originate, where third parties might be providing U.S.-based businesses with 24/7 services, etc.). Many laws (particularly for government entities and regulated industries) and lawyers' professional rules of responsibility expressly or by implication require appropriate data protection training for employees and sometimes contractors as well.[2]
- Command of the law is not enough, as businesses are often tried in the court of public opinion or are challenged by third-party watchdog groups, regardless of the current legality of the entity's practices.
- Likewise, technological innovation is occurring at a startling and accelerating pace. The Internet, mobile devices, and ever-more-sophisticated computer technology (all connected to each other and always on) make it easy to collect, analyze, combine, reproduce, and disseminate data, thereby enhancing efficiency and cost-effectiveness but also escalating the risk of making catastrophic mistakes at the speed of light. Yet employees often do not really understand that the latest "smart" technology at work or home (TVs, appliances, toys or gadgets, automated fish tanks, security cameras, digital assistants, voice-controlled smart home hubs, etc.) could be invisibly eavesdropping on confidential discussions using connected microphones, spying via built-in cameras, or providing a new attack vector for accessing the organization's digital assets.

Change is the watchword, and businesses and their cultures must be nimble in spotting trends and addressing issues that were not even on the radar screen months before.

Business leaders often breathe a sigh of relief once the state-of-the-art security system is installed and comprehensive data protection policies and

2. Please see Chapters 4 and 6 of this Handbook for further discussion about the types of legal and professional responsibility requirements placed on lawyers and law firms, which often include education and training.

procedures have been established. Yet notwithstanding adoption of the latest technology and sound data protection principles, businesses are only as strong as their weakest (human) link:

- The disgruntled or downsized "Gen X" employee who has it in for the organization and whose system access was not terminated on the last day of employment.
- The IT director who fails to install patches on a regular basis, thereby leaving networks vulnerable.
- The HR employee who leaves sensitive employee records unlocked or in electronic files with inadequate access restrictions.
- The associate who unwittingly compromises the firm's client relationships through a lost laptop, phone, or unencrypted flash drive left on an airplane or in a taxi or rideshare vehicle.
- The super-connected, tech-savvy "Millennial" employee who overshares on social media and underestimates how that may sabotage the company's confidential data.
- The road-warrior employee whose actions (or inaction) regarding the latest mobile technology (including "bring your own device") may violate internal data security policies or rules of professional responsibility.
- The "Baby Boomer" senior partner who unleashes ransomware by clicking on a link that looks like it came from a colleague or board member.
- The administrative assistant who provides extensive client or firm information after receiving a fraudulent e-mail that appears to be coming from her supervisor or a firm or business executive requesting information.
- The third-party vendor who stores data overseas without appropriate security controls.

Countless studies, audit trails, and surveys over the years have repeatedly confirmed that the biggest data protection threats come from within one's own organization. Most missteps are unintentional. Many mistakes can be avoided and risks can be minimized with appropriate training and awareness-raising. Yet this is often an overlooked component of data protection initiatives—the missing link when it comes to security.

B. What Does SMART Training Look Like?

What does training actually mean, and what are businesses doing to address data protection's weakest link? Over the years, this question has been posed to CPOs drawn from various industries, locations, and corporate cultures,[3] and a consistent pattern of answers has emerged. In short, when conducting training, businesses need to be SMART:

Start training on hiring.
Measure what you do.
Annually provide training.
Raise awareness and provide updates continually.
Tailor training by role.

In considering these SMART training steps and what they mean for one's business, it is important to keep in mind that the particular data protection training that is right for one entity is not necessarily right for another, even if they are in the same industry or are law firms of similar size. Businesses differ in many ways—for example, the degree of centralization, their corporate cultures, the jurisdictions in which they operate, their objectives, their resources and budget, their existing data protection infrastructure, their buy-in from senior management, and so on.

1. S—Start Training on Hiring

Given the fundamental role of data in everything a business does, training on how to protect that data should start on day one. Data protection training should be provided to all new employees and, increasingly, to contractors as well. In cases where it is not feasible to do such training for all employees initially (due to bandwidth, budget, or other constraints), businesses might choose to focus training on selected employees (e.g., HR personnel and those in key business roles or units).

3. Chapter co-author Ruth Hill Bro has posed such training questions since 2005 in her recurring column called *CPO Corner: Interviews with Leading Chief Privacy Officers,* which features 17 questions designed to identify trends and best practices, showcase the diverse range of CPOs, and capture key benchmarking and practical implementation information regarding data protection issues; see interviews posted at ABA, Section of Science & Technology Law: E-Privacy Law Committee, http:www.ambar.org/eprivacy.

In the employee context, training is provided as a part of employee orientation. Such training can take different forms, using a variety of media:

- An initial in-person, instructor-led session (large group, small group, or one-on-one, as appropriate), which can encourage interaction (but may not always be scalable or practical for some organizations in all situations), and/or
- An intranet/computer-based training module.

Coverage can include a wide range of topics, including:

- High-level overviews applicable to all employees and contractors;
- Instruction on relevant data protection laws and regulations (and professional rules of responsibility, where applicable), internal policies and procedures, fundamentals of the relevant technology, and industry best practices;
- Protecting confidentiality and security of data; and
- Steps to take when addressing a suspected data breach.

Such training should be coordinated with other training (regarding records management, code of conduct, etc.) and should be reviewed to avoid contradictions and conflicts in approach and message. Consideration should be given to whether the time, format, and content are suitable across different parts of the organization. Issues of translation, local law, and local customs can come into play here as well.

2. M—Measure What You Do

Measurement and assessment are a core component of many of these initial training sessions as well as in follow-up training. Administering tests (e.g., a graded online quiz) can help to confirm understanding and gauge the overall effectiveness of the training; it can also help to ensure that the work has actually been done. For example, employees and contractors could be required to correctly answer four of five assessment questions at the end of each training section. Broader measurements—such

as comparisons of incidents and types of missteps before and after training—can also help businesses to make training more effective while demonstrating return on investment (which can be important in making the case for budget).

3. A—Annually Provide Training

It is prudent (and in some cases required under applicable law, rules, or policies) to ensure that employees annually receive a data protection training update, along with corresponding assessments or tests. Where relevant, certification or continuing legal education (CLE) or professional responsibility credit could be provided, thereby offering an additional incentive to do the training. Such follow-up instruction is often computer-based, so it can be deployed to diverse geographic locations and in a time frame that is convenient for the person receiving the training. Sometimes these annual updates are a part of annual recertification regarding business conduct guidelines.

4. R—Raise Awareness and Provide Updates Continually

It is impossible to integrate appropriate data security practices into a culture by using just introductory training on hiring and mandatory annual training. To address this, businesses need to look for ways to raise data awareness and update employees on data protection on an ongoing basis. This is due to a number of factors, including the speed with which the issues change, the different ways in which people learn, the need for reinforcement, and so on. With ongoing awareness-raising, law firms and other businesses can integrate information security practices in such a way that they become as commonplace as turning on a computer.

5. T—Tailor Training by Role

Going beyond high-level, one-size-fits-all training allows for training to be tailored to focus on specific roles of individuals, different generational challenges, and specific requirements for contractors and third parties. Tailoring of data protection training can take various forms, depending on the organization:

- Start with a Data Protection 101 online course that is available on demand (successfully completing it results in a certificate). The basic module can then be supplemented by training and awareness-raising specific to role (HR, those involved heavily in data handling, contractors, product design, engineering, sales, senior executives, lawyers, paralegals, administrative assistants, etc.), business unit, geographic location, and the like.
- Determine who should receive direct training from, or at least meet in person with, the CPO, CISO, CIO or IT director, legal counsel, or other qualified trainers. It is helpful for those tasked with training to meet with selected employees to learn about their data practices and then tailor training efforts accordingly. For example, some CPOs meet regularly with the company's engineering, product design, and sales teams to raise important issues in planning meetings and gain insights to develop appropriate training.
- Ask data protection officers (or other relevant individuals) associated with the business lines to develop training and tools to enable the application of data protection policies to their respective areas.
- Hire specialists, internally or externally, to refine and enhance training efforts.
- Not all training and awareness-raising comes from within. Small firms or solo practitioners, those who lack specialized staff, and others looking for cost-effective approaches should take advantage of online training modules, relevant CLE courses and conferences, resources offered by bar associations (the American Bar Association and the ABA's Sections, Divisions, and Forums; state and local bar associations; specialty bar associations; etc.), training publications, and the like.
- As noted above, training for some roles (e.g., lawyers) may be accompanied by certification or CLE or professional responsibility credit.

Businesses that use SMART training can provide the missing link that will help make data protection a part of the culture and turn their employees into one of their strongest links when it comes to protecting one of the most valuable assets of any business.

II. SMART Training in Action

Implementing a SMART training program does not have to be complicated or require significant budget. The program pays for itself by reducing the risk of data loss and increasing awareness about data protection.

A. Understanding the Basics of Employees: Role and Generational Differences

First, any training program should assess and understand the recipients of the training. As mentioned above, the role of the employee in the organization will make a difference in the type of training received. An associate working with e-discovery matters and technology every day will have different considerations than a mail clerk or even other associates and partners in the firm.

In addition, generational differences play a role in how training should be developed, the type of training and communication that a person prefers to receive, and how best to provide the training. Cam Marston, in his practical and often humorous book *Generational Insights: Practical Solutions for Understanding and Engaging a Generationally Disconnected Workforce*,[4] discusses how each generation differs in its approach to learning:

- ***Baby Boomers*** (born 1946–1964) tend to continue to hold key leadership positions (e.g., partners) in the organization. They focus on work ethic and often measure it in terms of hours spent, rather than productivity. They value face time and relationships and seek loyalty. They look for those willing to put in whatever time is necessary to complete the task and support the team.[5] When training Baby Boomers, it is critical to include preevaluation of technology skills and training that is participatory but not intimidating.[6]
- ***Generation Xers*** (born 1965–1979) often have a more entrepreneurial spirit and are focused on challenging or reinventing the status quo.

4. Cam Marston, Generational Insights: Practical Solutions for Understanding and Engaging a Generationally Disconnected Workforce (2010).
5. *Id.* at 33–34.
6. *Id.* at 39.

They tend to seek open communication, no matter their title or status. Unlike Baby Boomers, Gen Xers focus on productivity rather than time. They often seek a person, not a company, where their loyalty will lie.[7] Training programs should address the Gen X employee's career goals and be flexible, providing options and choices. For Gen Xers to see training as valuable, senior-level management must demonstrate its commitment to the training as valuable.[8]

- ***Millennials*** (born 1980–2000) tend to be the most idealistic of the three groups. Unlike Gen Xers, who prefer to work independently with few checkpoints, Millennials want constant communication and positive reinforcement and prefer regular checkpoints at each phase of their work.[9] Training programs for Millennials need to be group-oriented (where practical), interactive, and fun. They prefer that everyone be allowed to take a role in some part of the teaching as well as the learning.[10]

Given the diverse nature of the workforce and the different means by which people learn and absorb information, any training or education campaign must integrate a variety of employee perspectives and capabilities and incorporate a variety of approaches.

B. Building an Effective and Diverse Program

Leveraging the **SMART** principles described above, any organization can quickly and easily build an ongoing training and education campaign.

First, it is critical to make the campaign fun and creative. While the message of data protection is serious, the delivery does not need to be. People of all generations tend to learn more through consistent messaging that has a direct impact on their lives. Those working on the data protection training should develop easy, fun, and catchy slogans that employees will remember.

7. *Id.* at 35.
8. *Id.* at 41.
9. *Id.* at 35, 37.
10. *Id.* at 42.

One example is the SAFE program,[11] an information security awareness program that was developed for Option Care Enterprises, Inc. as a way to help employees remember how best to protect and secure sensitive information:

Secure the organization's data: Where are you storing client data? How are you deleting it?

Asset protection: Do you know where your computer/iPad/phone is?

Friend or **F**oe: Who is sending you an e-mail? Is it something you expected or phishing?

Encrypt: Are you encrypting sensitive e-mails before sending them out?

A program such as SAFE can be used throughout the year to educate staff; different themes within each of the four SAFE categories above can be featured.

Next, identify something, such as a mascot, that represents the organization and symbolizes data protection to help lighten the delivery of a serious message. For example, Option Care, which provides infusion services to patients in their homes, uses a mascot named "The Infuser."

The Infuser's motto is "Infusing Security into Everything We Do." Every time employees see this mascot and message, they are reminded about protecting sensitive information. It is a fun, easy, and quick cue that costs very little to the organization to develop and implement.

Third, ensure that training is continuous, and use various methods to implement it. In addition to mandatory training at specific times (when employees join the organization and subsequent annual training), continuous education is key to any successful cultural transformation. The following are some ideas to keep the momentum going:

11. The SAFE program was developed by Option Care CISO Jill Rhodes, who is also an author of this chapter and co-editor of this Handbook. For further information on the program, contact Ms. Rhodes at jill.rhodes@optioncare.com.

- Leverage current newsletters, and place brief articles within them that discuss data protection.
- Conduct e-mail campaigns (monthly or as needed) with data protection guidelines, relevant media coverage, and so on to remind everyone (or otherwise make them aware) of relevant policies and practices.
- Offer periodic "Data Protection Awareness Weeks" or "Security Awareness Drives" with guest speakers and other special events.
- Strategically place wall posters and other communications that promote data protection.
- Publish monthly articles on the company and line-of-business intranet home pages to raise data protection awareness.
- Send periodic e-mails to highlight ongoing opportunities for online training and in-person sessions conducted by members of the data protection team or outside speakers.
- Develop white papers and other material related to relevant data protection topics (aiming for greater frequency and detail over time).
- Remind employees that data protection training is an important part of their job by including it as a factor in their annual performance evaluation; celebrate successes and reward those who meet the objectives (and, if needed, identify opportunities for growth and improvement).

Fourth, involve employees directly. Hold data protection competitions between divisions, offices, or floors in a building with the goal of identifying an employee/group activity that protected the organization's information in a noteworthy way. Recognize the individual or group winners, name them in the monthly newsletter or blog, and provide a pizza lunch for the winner—the more recognition, the better.

Build an ambassador/liaison or similar program across the organization. Whether it is by office, region, subject matter expertise, or business unit, identify a way to have a data protection representative in each. Although senior leadership is important, the representative should be a mid-level employee who still has influence with peers, subordinates, and leadership. Meet with the data protection ambassadors/liaisons regularly to discuss data protection issues and (in line with the discussion about Millennials above) ensure that they are a part of the solution by having them serve as

the leaders who will train and educate the employees they work with on a regular basis.

Educate employees about how to protect data at home as well as in the workplace. Data protection does not start when a person logs into the network or end when she shuts down for the evening. Everyone's family members and friends are constantly touching sensitive and/or personal digital data. Whether it is through social media or new mobile apps, data is being collected. By educating employees to protect data in all facets of their lives, they will approach data protection more holistically in their daily work life.

All of these methods are easy, cheap, fun, and effective ways to communicate and educate employees about enhancing data protection in the organization. As noted earlier, it is critical to find ways to measure the success of these campaigns (the "M" in "SMART" training).

C. Measuring Success (Through Phishing Campaigns and Other Means)

One of the easiest ways to measure the success of a campaign is to test employees by phishing them directly. Phishing normally occurs when a malicious e-mail is sent either directly to an individual (spear phishing) or to many in the hope that the target will click on a link within the e-mail and then spread a virus that could infect the individual's computer, at a minimum, or the entire enterprise network. Ransomware, discussed throughout this Handbook, has often been caused by phishing.

As part of a SAFE campaign (Friend or Foe), organizations can implement their own company-wide phishing campaign, sending "malicious" e-mails to employees, as someone trying to harm the organization would do. When an employee clicks on the e-mail, instead of infecting the system, the employee receives an educational message about the phishing e-mail and the fact that had it been real, harm could have come to the organization. This type of campaign measures the click rate and, when conducted regularly, can be used to monitor those who are clicking regularly. As a result, specific training can be developed for those individuals or groups. Phishing programs provide a quantitative measurement related to security awareness.

Reporting numbers also can provide both quantitative and qualitative opportunities for measuring success. As more training and education occurs, the number of incidents reported to appropriate leadership will also increase.

Increased reporting could be anything from the reporting of a specific data breach or loss incident to reporting of phishing e-mails. As these incidents are tracked, greater information becomes available about employee knowledge and understanding of data protection.

In the end, a data breach or loss will most likely occur as a result of something an employee did or did not do. The best way to prevent such missteps is to educate the people in the organization about how they can better protect the information around them.

III. Ten Key Points

1. Make data protection a part of the corporate culture and the job of every individual.
2. Recognize that the biggest risks to data come from the people working for the organization and that training and raising awareness are essential to reducing those risks.
3. Be SMART in training: Start training on hiring. Measure what you do. Annually provide training. Raise awareness and provide updates continually. Tailor training by role.
4. Recognize that one size doesn't fit all; it is important to undertake training that fits a business's own needs.
5. Build a program that represents the organization's employees both from a role perspective and a generational one.
6. Make any training campaign fun and interesting—let the employees lead it through ambassador/liaison programs and in other ways.
7. Train employees on how to protect information in all facets of their lives, not just in the workplace. By helping them protect their family and friends at home, they will further integrate these practices at work.
8. Reward! Reward! Reward! Use competitions with prizes to further induce employees to become more aware and supportive of data protection across the organization.
9. Measure success through phishing programs and tracking of reporting of incidents and responses.

10. Know that training and awareness-raising is a never-ending journey (not a destination) that can require changes in direction in response to changes in the law, technology, media coverage, and one's own experiences and new business initiatives. Adapt accordingly, while keeping message delivery mechanisms light and easy to understand for all of the people who work for the organization.

Chapter 4

Lawyers' Legal Obligations to Provide Data Security

Thomas J. Smedinghoff and Ruth Hill Bro

Virtually all of the daily transactions and key records of a business (whether a law firm, corporation, public interest entity, or the like) are created, used, communicated, and stored in electronic form using networked computer technology. Although such technology provides the business with tremendous economic benefits, including reduced costs and increased productivity, it also creates significant potential vulnerabilities that can adversely affect the business, its clients and customers, and other entities with whom it interacts.

Creating, using, communicating, and storing information in electronic form greatly increases the potential for unauthorized access, use, disclosure, alteration, loss, or destruction of the information. Front-page news stories about data security missteps made by companies, government agencies, and other businesses (including law firms) are a testament to the growing significance of this problem and should serve as a wake-up call for lawyers in all practice settings. Insert your firm's name, or your client's name, in the most recent data breach headline, and the risk of not taking sufficient security steps (especially those that are legally required) becomes all too real.

I. Overview

A. What Is Data Security?

The concept of "security" refers to an entity's implementation and maintenance of *security controls* to protect one or more of its *assets* (such as

buildings, equipment, cargo, inventory, and people) from *threats*. Information security (also referred to as "cybersecurity" or "data security") involves the implementation of security controls to protect a business's *digital assets*. It has been generally described as "the protection of *information and information systems* from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."[1] Thus, information security involves the protection of both (1) *information systems*—that is, computer systems, networks, and software—and (2) the *electronic records*, *data*, *messages*, *and other information* that are typically recorded on, processed by, communicated via, stored in, shared by, or received from such information systems.

The *objectives* of using security measures can be defined in terms of either the positive results to be achieved or the negative consequences to be avoided. The positive results to be achieved are typically described as ensuring the *confidentiality*, *integrity*, and *availability* of information.[2] The harms to be avoided, as noted above, are often described as unauthorized access, use, disclosure, disruption, modification, or destruction.[3]

Achieving these objectives involves implementing security measures designed to protect systems and information from the various threats they face. The kinds of threats, where they come from, what is at risk, and the seriousness of the consequences will, of course, vary greatly from case to case. But responding to those threats with appropriate security measures is the focus of the duty to provide security.

Measures designed to protect the security of information systems and data are generally grouped into the following three categories (based on the nature of the control):

1. NIST, NISTIR 7298, Rev. 2, Glossary of Key Information Security Terms 94 (May 2013) (definition of "information security") (emphasis added). *See also* Federal Information Security Management Act (FISMA), 44 U.S.C. § 3542(b)(1) (definition of "information security").

2. *See, e.g.*, FISMA, 44 U.S.C. § 3542(b)(1); Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Regulations, 45 C.F.R. § 164.306(a)(1).

3. *See supra* note 1.

- ***Physical security controls.*** These security measures are designed to protect the tangible items that comprise the physical computer systems, networks, and storage devices that process, communicate, and store the data, including servers, devices used to access the system, storage devices, and the like. Physical security controls are intended to prevent unauthorized persons from entering that environment and to help protect against natural disasters. One regulation defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."[4] Examples of physical security controls include fences, walls, and other barriers; locks, safes, and vaults; armed guards; sensors; and alarm bells.
- ***Technical security controls.*** These security measures typically involve the use of software and data safeguards incorporated into computer hardware, software, and related devices. These measures are designed to ensure system availability, control access to systems and information, authenticate persons seeking access, protect the integrity of information communicated via and stored on the system, and ensure confidentiality where appropriate. Examples include firewalls, intrusion detection software, access control software, antivirus software, passwords, PIN numbers, smart cards, biometric tokens, and encryption processes.
- ***Administrative security controls.*** Sometimes referred to as "procedural" or "organizational" controls, these security measures consist of written policies, procedures, standards, guidelines, and supplemental administrative controls to guide conduct, prevent unauthorized access, and provide an acceptable level of protection for computing resources and data. Administrative security measures frequently include personnel management, employee use policies, training, discipline, and informing people how to conduct day-to-day operations.

4. HIPAA Security Regulations, 45 C.F.R. § 164.304.

Within each of these three categories, security measures are further classified into the following three separate categories (based on their timing regarding the risks and threats they are designed to address):

- ***Preventive*** security measures are designed to prevent the occurrence of events that compromise security. Examples include a lock on a door (to prevent access to a room containing computer equipment) or a firewall (to prevent unauthorized online access to a computer system).
- ***Detective*** security measures are designed to identify security breaches after they have occurred. Examples include a smoke alarm (to detect a fire) or intrusion detection software (to detect and track unauthorized online access to a computer system).
- ***Reactive*** security measures are designed to respond to a security breach and typically include efforts to stop or contain the breach, identify the party or parties involved, and allow recovery of information that is lost or damaged. Examples include calling the police (after an alarm detects that a burglary is in process) or shutting down a computer system (after intrusion detection software determines that an unauthorized user has obtained access to the system).

B. Security Law: The Basic Security Obligations

Concerns about individual privacy, accountability for financial information, the authenticity and integrity of transaction data, and the need to protect the confidentiality and security of sensitive business and client data are driving the enactment of new laws and regulations designed to ensure that all businesses adequately address the security of the data in their possession or under their control. Taken as a group, those laws and regulations impose two fundamental obligations on most businesses:

- The duty to provide security for their data; and
- The duty to warn of security breaches that occur.

The thesis of this chapter is that all businesses (including law firms), whether regulated or not, are generally subject to these legal duties regarding the security of the data in their possession or under their control. The following sections explain the source and scope of those duties.

II. The Duty to Provide Data Security

A. What Is the Duty?

The law often simply refers to the basic legal duty to provide data security as an obligation to implement "reasonable" or "appropriate" security measures designed to ensure the *confidentiality*, *integrity*, and *availability* of information. For example, several state security laws, such as in California, generally impose a duty to implement "*reasonable* security procedures and practices."[5] At the federal level, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires "*reasonable and appropriate*" security,[6] and the Gramm-Leach-Bliley (GLB) security regulations require security "*appropriate* to the size and complexity of the bank and the nature and scope of its activities."[7]

The focus on the reasonableness or appropriateness of security makes clear that the law recognizes that security is a relative concept: what qualifies as reasonable or appropriate security varies with the situation. Thus, the law typically provides little or no guidance on what specific security measures are required or on how much security a business should implement to satisfy those legal obligations. Although some laws include specific requirements for particular security measures that must be implemented,[8] the laws generally provide no safe harbors. Accordingly, the choice of security measures and technology can vary depending on the situation.

B. To Whom Does the Duty Apply?

Generally, the duty to provide security applies to all businesses, including law firms.

Certain sectors of the U.S. economy are, of course, subject to extensive regulations regarding data security. The most obvious examples are the

5. Cal. Civ. Code § 1798.81.5(b) (emphasis added).

6. 42 U.S.C. § 1320d-2(d)(2) (emphasis added).

7. 12 C.F.R. pt. 208, app. D-2, pt. II.A (Federal Reserve System) (emphasis added). *See also* other GLB-implementing security regulations: 12 C.F.R. pt. 30, app. B, pt. II.A (OCC); 12 C.F.R. pt. 364, app. B, pt. II.A. (FDIC); and 16 C.F.R. § 314.3(a) (FTC) (adding "sensitivity of any customer information at issue" to the other factors in determining what is "appropriate").

8. For example, the Massachusetts security regulations require implementation of firewalls, the use of virus software, and, in certain cases, the use of encryption. *See* 201 Mass. Code Regs. 17.00.

financial sector,[9] the healthcare sector,[10] the federal government sector,[11] and other critical infrastructure sectors.[12] But there also is no doubt that unregulated businesses are subject to data security obligations.

One need look no further than the last 15 years of Federal Trade Commission (FTC) enforcement actions, as well as recent state attorney general enforcement actions, to see that numerous nonregulated businesses have been targeted for failing to provide appropriate security for their own data. Examples include software vendors (Oracle, Microsoft, Guidance Software), consumer electronics companies (ASUS, TRENDnet, HTC America, Genica/Computer Geeks), mobile app developers (Snapchat, Fandango, Credit Karma), clothing/shoe retailers (Guess, Life is Good, DSW), music retailers (Tower Records), animal supply retailers (Petco), general merchandise stores (Target, BJ's Wholesale, TJX Companies), restaurant and entertainment establishments (Dave & Busters, Briar Group), social media and networking sites (Twitter, Facebook, and Ashley Madison), transcription services (GMR), bookstores (Barnes & Noble), property management firms (Maloney Properties, Inc.), and hotels (Wyndham).[13]

In addition to the federal- and state-level unfair or deceptive trade practice statutes that often support these enforcement actions, many state security laws and regulations expressly apply to "any business" or "any person" that maintains certain types of data. Of course, this includes law firms.

Moreover, as discussed below, many sector-specific security regulations may be imposed on law firms through their client relationships. For example, the HIPAA regulations in the healthcare sector and the GLB

9. Subject to GLB, Pub. L. No. 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing security regulations; *see supra* note 7.

10. Subject to HIPAA, 42 U.S.C. § 1320d-2, and HIPAA Security Regulations, 45 C.F.R. pt. 164.

11. Subject to FISMA, 44 U.S.C. §§ 3541–3549.

12. *See* Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739 (Feb. 19, 2013), *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

13. *See, e.g.*, FTC, Data Security, https://www.ftc.gov/datasecurity (for list of all FTC data security cases and enforcement actions); May 2017 state attorneys general settlement agreement with Target Corp., http://www.illinoisattorneygeneral.gov/pressroom/2017_05/17-AVC-0008TargetCorporation.pdf.

regulations in the financial sector both require that entities governed by those regulations push down certain security obligations to their service providers (which includes law firms) who access the protected data. In addition, the HIPAA regulations have been revised to impose security obligations directly on "covered entities" providing services to healthcare companies.

C. What Is the Source of the Duty?

There is no single law, statute, or regulation that governs the obligations of a business or law firm to provide security for the information in its possession or under its control. Instead, legal obligations to implement data security measures are found in an ever-expanding patchwork of state, federal, and international laws, regulations, and enforcement actions, as well as in common-law duties and other express and implied obligations to provide "reasonable" or "appropriate" security for business data.

Some laws seek to protect the business and its owners, shareholders, investors, and business partners. Other laws focus on the interests of employees, customers, and prospects. In some cases, governmental regulatory interests or evidentiary requirements are at stake. Many of the requirements are industry-specific (e.g., focused on the financial sector or the healthcare sector) or data-specific (e.g., focused on personal information or financial data). Some laws focus only on public companies.

When viewed as a group, however, such laws and regulations provide ever-expanding coverage of most business activity. The most common sources of obligations to provide security include the following:

Statutes and Regulations.[14] Numerous statutes and regulations impose obligations to provide data security. Sometimes these statutes and regulations use recognizable terms such as "security" or "safeguards," but in many cases they are subtler by using attributes of security, such as

14. *See* Appendices A (Federal Statutes), B (State Statutes), C (Federal Regulations), and D (State Regulations) of this Handbook for examples of such statutes and regulations. See also Appendices H (CFPB Decision and Consent Decree), I (FTC Decisions and Consent Decrees), and J (SEC Decision and Consent Decree) for government enforcement actions under certain statutes and regulations.

"authenticate," "integrity," "confidentiality," "availability of data," and the like. Such statutes and regulations include the following:

- ***Privacy laws and regulations***, which typically include provisions governing the security of the personal data covered by the applicable law.
- ***Security laws and regulations***, such as the state-level security laws that impose a general obligation on businesses to protect the security of certain personal data they maintain about individuals and/or that regulate the communication or destruction of certain data;
- ***E-transaction laws***, which are designed to ensure the enforceability and compliance of electronic documents generally;
- ***Corporate governance legislation and regulations***, which are designed to protect public companies and their shareholders, investors, and business partners;
- ***Unfair business practice laws***, at both the federal and state level, and precedent set by related government enforcement actions; and
- ***Sector-specific regulations***, such as the HIPAA security regulations and the GLB Safeguard Rules, which impose security obligations regarding specific data in the healthcare and financial sectors, respectively.

Common-Law Obligations.[15] For years, commentators have argued that there is a common-law duty to provide appropriate security for corporate and personal data, the breach of which constitutes a tort. Courts are beginning to accept that view. In one case, for example, the court held that "defendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information."[16] In another case of particular significance to lawyers, the court allowed plaintiffs to proceed on a "negligent misrepresentation" claim based on the theory that the defendants made implied representations that they had implemented the security measures required by industry practice to safeguard personal and financial information.[17]

15. *See, e.g.*, selected cases listed in Appendix G (Court Decisions re Duty to Provide Data Security) of this Handbook.

16. Bell v. Mich. Council, 205 Mich. App. LEXIS 353, at *16 (Mich. App. Feb. 15, 2005).

17. *In re* TJX Cos. Retail Sec. Breach Litig., 524 F. Supp. 2d 83 (D. Mass. 2007).

Rules of Evidence. Providing appropriate security to ensure the integrity of electronic records (and the identity of the creator, sender, or signer of the record) can be critical to securing the admission of an electronic record in evidence in a dispute. This conclusion is supported by the form requirement for an "original" in electronic transaction laws,[18] the evidence rules regarding authentication,[19] and case law addressing evidentiary authentication requirements.[20]

Rules of Professional Responsibility. Lawyers are, of course, subject to rules of professional responsibility. Such rules generally are patterned after the ABA Model Rules of Professional Conduct, which were modified in August 2012 by the ABA Commission on Ethics 20/20 to provide updated guidance regarding lawyers' use of technology and confidentiality obligations.[21]

Contractual Obligations. Businesses frequently try to satisfy (at least in part) their obligation to protect data by entering contracts with third parties who will possess, or have access to, their business data. This is particularly common in outsourcing agreements where the data will be processed by a third party. Several laws, such as the generally applicable Massachusetts data security regulations[22] or the financial sector's GLB Safeguard Rules, mandate that the business impose appropriate security obligations on the third party with access to its data. In other cases, businesses must comply with the requirements of certain technical security standards. Examples include the Payment Card Industry Data Security Standard (PCI Standard),[23] to which merchants must agree as a condition of accepting credit cards.

---

18. *See, e.g.*, Unif. Electronic Transactions Act (UETA) § 12(d), http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf; Electronic Signatures in Global and National Commerce Act (E-SIGN) 15 U.S.C. § 7001(d)(3), *available at* https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.

19. *See, e.g.*, Fed. R. Evid. 901(a).

20. *See, e.g.*, Am. Express v. Vinhnee, 336 B.R. 437 (B.A.P. 9th Cir. 2005); Lorraine v. Markel, 241 F.R.D. 534 (D. Md. May 4, 2007).

21. These rules and other law applicable specifically to lawyers are covered in Chapter 6 of this Handbook.

22. Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 Mass. Code Regs. 17.00 *et seq.* (2012) [hereinafter Mass. Standards for the Protection of Personal Info], *available at* http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

23. *See* PCI Sec. Standards Council, https://www.pcisecuritystandards.org.

Self-Imposed Obligations. In many cases, security obligations are self-imposed. Through statements in privacy notices, on websites, in advertising materials, or elsewhere, businesses often make representations regarding the level of security they provide for their data (particularly personal data collected from persons to whom the statements are made). By making such statements, businesses impose on themselves an obligation to comply with the standard they have told the public that they meet. If those statements are not true, or are misleading, they may become deceptive trade practices under section 5 of the FTC Act or equivalent state laws.

Obligations Pushed Down from Clients. In some cases, data security laws and regulations do not apply directly to law firms, but might apply indirectly (e.g., because of law firm clients who themselves are subject to certain sector-specific security regulations). Such regulations frequently impose on covered businesses an obligation to push down certain security requirements to third parties with whom they do business or who otherwise are involved in processing their data. This approach is increasingly becoming a source of data security obligations for law firms. For example, a law firm must comply with security requirements imposed on its financial or healthcare sector clients where those requirements must be passed down to the law firm. In many such cases, client requirements to satisfy certain security regulations motivate client audits of law firm security measures.

Thus, the duty of any business (and any law firm) to provide security may come from several different sources and several different jurisdictions—each perhaps regulating a different aspect of the business's information—but the net result is a general obligation to provide security for all business data and information systems. In other words, information security is not just good business practice; it is a legal obligation.

D. What Data Is Covered?

All types of law firm and client business information should be protected by appropriate security; such information includes financial information, personal information, tax-related records, employee information, transaction information, information obtained from or produced for clients, litigation information (including what is obtained in discovery), and other confidential information.

When examining particular security laws that may apply to a business or a law firm, it is important to note that such laws will frequently focus on a certain category of information. Commonly addressed categories include the following:

- ***Attorney-client data.*** Any client-related data held by the law firm is likely to be subject to numerous legal obligations to protect the security of that data. In addition to the legal obligations discussed here (which may be imposed directly on the law firm, or indirectly by clients obligated to push down their own imposed obligations), lawyers also have ethical obligations to protect client data.[24]
- ***Personal data.*** The obligation to provide adequate security for personal data collected, used, communicated, or stored by a business is a critical component of all privacy laws as well as sector-specific privacy regulations, such as those governing healthcare or personal financial records.
- ***Financial data.*** Corporate governance laws designed to protect the company and its shareholders, investors, and business partners (such as Sarbanes-Oxley and implementing regulations) require public companies to ensure that they have implemented appropriate information security controls for their financial information.[25] Similarly, Securities and Exchange Commission (SEC) regulations impose various requirements for internal controls over information systems.
- ***Transaction records.*** Both the federal and state electronic transaction statutes—Electronic Signatures in Global and National Commerce Act (E-Sign) and the Uniform Electronic Transactions Act (UETA), now enacted in 47 states, the District of Columbia, and the U.S. Virgin Islands)—require security for storage of electronic records relating to online transactions.

24. *See* Chapter 6 of this Handbook.

25. *See generally* Bruce H. Nearon et al., *Life after Sarbanes-Oxley: The Merger of Information Security and Accountability*, 45 Jurimetrics: J.L., Sci. & Tech. 379–412 (Summer 2005).

- ***Tax records.*** Internal Revenue Service (IRS) regulations require businesses to implement information security to protect electronic tax records and as a condition of engaging in certain electronic transactions.
- ***E-mail.*** SEC regulations address security in a variety of contexts, and Food and Drug Administration (FDA) regulations require security for certain records.

Most laws do not differentiate based on the format of the data involved. Data kept in databases, e-mails, text documents, spreadsheets, voicemail messages, pictures, video, sound recordings, and other formats is typically treated the same.

In some cases, however, statutes and regulations governing data security differ based upon the media on which the data resides. Many laws focus only on electronic forms of data. Some, however, also address paper-based information (e.g., including those regulating proper data destruction). Some rules also can become very media-specific. For example, under some regulations, data kept on "removable media" is subject to additional encryption requirements that do not apply to data stored on other forms of electronic media.

E. What Level of Security Is Required?

Defining the scope of a lawyer's security obligations begins with understanding that the law views security as a relative concept. Thus, as noted above, the basic standard for compliance is typically that security must be "reasonable"[26] or "appropriate."[27]

---

26. *See, e.g.*, HIPAA, 42 U.S.C. § 1320d-2, and HIPAA Security Regulations, 45 C.F.R. § 164.306; COPPA, 15 U.S.C. § 6502(b)(1)(D), and COPPA regulations, 16 C.F.R. § 312.8; I.R.S. Rev. Proc. 97-22, sec. 4.01(2); SEC regulations, 17 C.F.R. § 257. *See also* UCC art. 4A, § 202 ("commercially reasonable" security procedure). Although HIPAA requires "reasonable *and* appropriate" security, 42 U.S.C. 1320d-2(d)(2) (emphasis added), some state personal information security laws require only that security procedures and practices be "reasonable"—*e.g.*, CAL. CIV. CODE § 1798.81.5(b). *See also* Appendix B.1 (State Laws Imposing Obligations to Provide Security for Personal Information) of this Handbook.

27. HIPAA requires "reasonable and appropriate" security, 42 U.S.C. 1320d-2(d)(2). GLB requires covered financial institutions to "implement a comprehensive written information security program that includes administrative, technical, and physical safeguards *appropriate* to the size and complexity of the bank and the nature and scope of its activities." 12 C.F.R. pt. 208, app. D-2, pt. II.A (Federal Reserve System) (emphasis added); *see also* GLB-implementing security regulations, *supra* note 7. The Massachusetts data security regulations require a comprehensive

In some cases, statutes and regulations define that standard in terms of positive results to be achieved, such as ensuring the *confidentiality*, *integrity*, and *availability* of systems and information.[28] In other cases, that standard is defined in terms of the harms to be avoided—for example, to protect systems and information against unauthorized access, use, disclosure, and so on. In some cases, the standard is not defined.

Regardless of approach, meeting this standard and achieving these objectives involves implementing appropriate physical, technical, and administrative security measures to protect both information systems and information from the various threats they face. Because those threats vary greatly from business to business, laws and regulations rarely specify or provide guidance about what specific security measures or technology a business should implement,[29] but instead require establishing and maintaining internal security "procedures," "controls," "safeguards," or "measures"[30] designed to achieve the objectives identified above.

F. The Legal Requirements for "Reasonable Security"

Although security is relative, a legal standard for "reasonable" security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.

---

written security program that contains safeguards that are "appropriate" to the size of the business, the resources available, the amount of stored data, and the need for security. Mass. Standards for the Protection of Personal Info., 201 Mass. Code Regs. 17.03(1).

28. *See, e.g.*, FISMA and HIPAA Security Regulations, *supra* note 2. *See also* GLB Security Regulations (OCC), 12 C.F.R. pt. 30, app. B, pt. II.B; Mass. Standards for the Protection of Personal Info., 201 Mass. Code Regs. 17.00; N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23, § 500.02.

29. Laws and regulations, however, do often focus on categories of security measures to address. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. pt. 164. *See also* Appendices E (Best Practice Guidelines Issued by Federal Government Agencies) and F (Best Practices Guidelines Issued by State Government Agencies) of this Handbook.

30. *See, e.g.*, FDA regulations at 21 C.F.R. pt. 11 (procedures and controls); SEC regulations at 17 C.F.R. 257.1(e)(3) (procedures); SEC regulations at 17 C.F.R. 240.17a-4 (controls); GLB regulations (FTC) 16 C.F.R. pt. 314 (safeguards).

This "process-oriented" legal standard for information security has been widely adopted:

- It was first outlined in a series of financial industry security regulations required under GLB titled Interagency Guidelines Establishing Standards for Safeguarding Consumer Information. They were issued by the Federal Reserve, the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision on February 1, 2001,[31] and later were adopted by the FTC in its Safeguards Rule on May 23, 2002.[32]
- The same approach was incorporated in the Federal Information Security Management Act of 2002[33] (FISMA) and in the HIPAA Security Standards issued by the Department of Health and Human Services on February 20, 2003.[34]
- The FTC has since adopted the view that the "process-oriented" approach to information security outlined in these regulations is a "best practice" for legal compliance that should apply to all businesses in all industries. The FTC has, in effect, implemented this "process-oriented" approach in all of its decisions and consent decrees relating to alleged failures to provide appropriate information security.[35]
- The National Association of Insurance Commissioners (NAIC) has recommended the same approach, and several state insurance regulators have adopted it.[36]

31. 12 C.F.R. pt. 30, app. B (OCC), 12 C.F.R. pt. 208, app. D-2 and 12 C.F.R. pt. 25, app. F (Federal Reserve System), 12 C.F.R. pt. 364, app. B (FDIC), 12 C.F.R. pt. 568 and 570, app. B (Office of Thrift Supervision, which merged with the OCC as of July 21, 2011)).

32. FTC, Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484 (May 23, 2002) (FTC Safeguards Rule); 16 C.F.R. pt. 314.

33. 44 U.S.C. § 3544(b).

34. 45 C.F.R. pt. 164.

35. *See, e.g.*, FTC, Data Security, https://www.ftc.gov/datasecurity (listing FTC data security cases and corresponding decisions and consent decrees implementing this approach).

36. *See, e.g.*, Nat'l Ass'n of Ins. Comm'rs, ST-673-1, Standards for Safeguarding Customer Information Model Regulation (Apr. 2002), http://www.naic.org/store/free/MDL-673.pdf. See other NAIC cybersecurity resources at http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

- The Illinois Attorney General[37] endorsed this approach in 2012; the California Attorney General[38] did likewise in 2016.
- Some courts are taking the same approach.[39]
- The Massachusetts Office of Consumer Affairs and Business Regulation adopted the approach in 2008 when it released its "Standards for Protection of Personal Information of Residents of the Commonwealth"[40] (Massachusetts Regulations), as required by the 2007 Massachusetts security breach and data destruction law.[41] By specifically requiring businesses to implement a risk-based, process-oriented, comprehensive written information security program in accordance with a detailed list of requirements, the Massachusetts Regulations created one of the most comprehensive sets of general data security obligations imposed on businesses by a state.
- The 2017 cybersecurity regulations released by the New York State Department of Financial Services also adopted a similar approach.[42]

The trend in the law is to recognize what security consultants have been saying for some time: "security is a process, not a product."[43] Legal compliance with security obligations involves applying a "process" to the facts of each case to achieve an objective (i.e., to identify and implement the security measures appropriate for that situation), rather than implementing specific security measures in all cases. Thus, law firms cannot simply implement a

37. Ill. Att'y Gen., Information Security and Security Breach Notification Guide 5 (Jan. 2012), http://www.illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guidance.pdf.

38. Cal. Att'y Gen., California Data Breach Report 2016, at 29 (Feb. 2016), https://oag.ca.gov/breachreport2016.

39. *See, e.g.*, Guin v. Brazos Higher Educ. Serv., 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006).

40. Mass. Standards for the Protection of Personal Info., 201 Mass. Code Regs. 17.00 *et seq*.

41. Mass. Gen. Laws ch. 93H, § 2(a).

42. N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23. § 500.02.

43. Bruce Schneier, Secrets & Lies: Digital Security in a Networked World, at xii (2000). *See also* Appendices E (Best Practice Guidelines Issued by Federal Government Agencies) and F (Best Practices Guidelines Issued by State Government Agencies) of this Handbook.

standard set of security controls but rather must look more closely at their own individual situation.

This process-oriented approach to security compliance generally requires all businesses (including law firms) to take several steps, as outlined below.

1. Identify Information Assets

To protect something, you must know what it is, where it is, how it is used, how valuable it is, and so forth. Thus, when addressing information security, the first step is to identify the information assets to be protected and define the scope of the effort. This involves taking an inventory of the data that the business creates, collects, receives, uses, processes, stores, and communicates to others. It also requires examining the systems, networks, and processes by which such data is created, collected, received, used, processed, stored, and communicated.

Sensitive data files are often found in a variety of places within the firm. Data also is often in the possession and control of a third party, such as an outsource service provider or cloud provider. Yet the business (or law firm) is still responsible for the security of its (or its clients') data in the possession of third parties.

Identifying information assets also will help to determine the data security laws and regulations applicable to specific assets that must be addressed. This includes, for example, protected health information regulated under HIPAA, personally identifiable financial information regulated under GLB, information about children regulated under the Children's Online Privacy Protection Act (COPPA), and other types of personal information regulated under state security laws, the Fair Credit Reporting Act, or section 5 of the FTC Act.

Many security laws, regulations, and guidance documents expressly require identification of information assets. Examples include the following:

- An FTC business guidance document states what should be obvious but is often overlooked: "Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to

assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows."[44]

- A California attorney general guidance document states that organizations should "[i]dentify information assets and data to be secured."[45]
- Identification of information assets is a key component of the Cybersecurity Framework of the National Institute of Standards and Technology (NIST) and is included in the "Identify" function and "Asset Management" category of the Framework Core.[46]

2. *Conduct Periodic Risk Assessments*

Just as you cannot implement security until you identify what you have that needs to be protected, you also cannot implement security until you know what risks you need to protect against. Thus, implementing reasonable security to protect the information assets of a business requires a thorough assessment of the potential risks to the entity's information systems and data.

A *risk assessment* is the process of identifying vulnerabilities and threats to the information assets used by the business or firm and assessing the potential impact and harm that would result if a threat materializes. This forms the basis for determining what countermeasures (i.e., security controls), if any, should be implemented to reduce risk to an acceptable level. Thus, a risk assessment requires:

- Conducting a threat assessment to identify all reasonably foreseeable internal and external *threats* to the information and system assets to be protected;[47]

44. FTC, Protecting Personal Information: A Guide for Business 2 (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

45. *See* Cal. Att'y Gen., California Data Breach Report 2016, at 29 (Feb. 2016), https://oag.ca.gov/breachreport2016.

46. NIST Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) [hereinafter Cybersecurity Framework], Framework Core at app. A, https://www.nist.gov/cyberframework. The Cybersecurity Framework is discussed in section II.H below.

47. *See, e.g.*, GLB Security Regulations, 12 C.F.R. pt. 30, app. B, pt. III.B.1.

- Conducting a *vulnerability* assessment to identify the organization's vulnerabilities;
- Assessing the *likelihood* that each of the threats will materialize and, if so, the probability that one or more of the vulnerabilities will be exploited to cause harm—that is, identifying the likelihood that threat sources with the potential to exploit weaknesses or vulnerabilities in the system will actually do so;
- Evaluating the potential *damage* that will result; and
- Assessing the sufficiency of the security controls in place to guard against the threat.[48]

A *threat* is anything that has the potential to cause harm. It can be an act of nature (such as a fire, flood, or tornado) or man-made, such as a computer virus, a hacker's actions, or an employee's negligent mistake. Threats should be considered in each area of relevant operation, including information systems; network and software design; information processing, storage, and disposal; prevention, detection, and response to attacks, intrusions, and system failures; and employee training and management.

Assessing risks also requires consideration of vulnerabilities. A *vulnerability* is a flaw or weakness that can be accidentally triggered or intentionally exploited by the threat to endanger or cause harm to an information asset. A vulnerability might be a hole in the roof, a system with easy-to-guess passwords, unencrypted data on a laptop computer, disgruntled employees, or employees who simply do not understand what steps they need to take to protect the security of the firm's data.

The likelihood that a threat will exploit a vulnerability to cause harm creates a *risk*. In other words, *risk* is the likelihood that something bad will happen that causes harm to an information asset. Somewhat more precisely, "[r]isk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the

48. *See, e.g.*, FISMA, 44 U.S.C. § 3544(a)(2)(A) and 3544(b)(1); GLB Security Regulations, 12 C.F.R. pt. 30, app. B, pt. III.B.2.

likelihood of occurrence."[49] Risk is present wherever a threat intersects with a vulnerability. For example, if the threat is rain, and the vulnerability is a hole in the roof, risk is the likelihood that it will rain, causing water to enter the building through the hole in the roof and doing damage to the building and/or its contents. Similarly, if the threat is a hacker, and the vulnerability is open Internet access to a server containing sensitive data, risk is the likelihood that a hacker will enter the system and view, copy, alter, or destroy the sensitive data.

This process will be the baseline against which security controls can be selected, implemented, measured, and validated. The goal is to understand the risks that the firm faces, to determine which risks are acceptable, and to identify appropriate and cost-effective safeguards to combat the risks that are unacceptable. Thus, such risks should be evaluated in light of the nature of the business or law firm and its clients, its transactional capabilities, the sensitivity and value of the stored information to the business and its trading partners, and the size and volume of its transactions.[50]

Numerous security laws and regulations expressly require a risk assessment as part of a comprehensive security program. Laws and regulations that do not expressly include such a requirement often do so implicitly.

- Various federal security statutes and regulations, including GLB,[51] HIPAA,[52] and FISMA,[53] expressly require a risk assessment.
- The consent decrees entered in FTC enforcement actions have expressly required "the identification of material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information."[54]

49. NIST Spec. Publ'n 800-30, Rev. 1, Guide for Conducting Risk Assessments 8 (Sept. 2012).

50. *See, e.g.*, Fed. Fin. Insts. Examination Council, Authentication in an Electronic Banking Environment 3 (July 30, 2001), https://www.ffiec.gov/pdf/authentication_guidance.pdf.

51. 16 C.F.R. § 314.4(b).

52. 45 C.F.R. § 164.308(a)(1)(ii)(A).

53. 44 U.S.C. 3554(b)(1).

54. *See* FTC, Data Security, https://www.ftc.gov/datasecurity (listing FTC cases and enforcement actions alleging failure to provide reasonable security).

- State security laws (e.g., in Oregon[55]) and regulations in Massachusetts[56] and New York[57] expressly require a risk assessment.
- Risk assessment is a key component of the NIST Cybersecurity Framework and is included in the "Identify" function and "Risk Assessment" category of the Framework Core.[58]
- The California attorney general's office released a report stating that "[i]nformation security laws and regulations generally require a risk management approach. In essence, this means organizations must develop, implement, monitor, and regularly update a comprehensive information security program [under which organizations must] assess risks to the assets and data."[59]
- Similarly, guidance issued by the Illinois attorney general recommends that businesses and government agencies should "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks."[60]
- In addition, several U.S. courts have held that a risk assessment plays a key role in determining whether a duty will be imposed and liability found. Where injury is foreseeable and preventable, a business has a duty to provide appropriate security to address the potential harm.[61] On the other hand, where a proper risk assessment was done, but a

55. Or. Rev. Stat. § 646A.622(2)(d)(A).

56. Mass. Standards for the Protection of Personal Info., 201 Mass. Code Regs. 17.03(2)(b).

57. N.Y. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services Companies, N.Y. Comp. Codes R. & Regs. tit. 23, § 500.02.

58. *See* Cybersecurity Framework, *supra* note 46, § 1.2 and Framework Core at app. A.

59. Cal. Att'y Gen., California Data Breach Report 2016, at 29 (Feb. 2016) https://oag.ca.gov/breachreport2016.

60. Ill. Att'y Gen., Information Security and Security Breach Notification Guide 5 (Jan. 2012), http://www.illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guidance.pdf.

61. *See, e.g.*, Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007); Bell v. Mich. Council, 2005 Mich. App. LEXIS 353 (Mich. App. Feb. 15, 2005).

particular harm was not reasonably foreseeable, the defendant would not be liable for failure to defend against it.[62]

The following publications provide general information and guidance on conducting a risk assessment:

- NIST Special Publication 800-30, Rev. 1, *Guide for Conducting Risk Assessments*[63]
- Massachusetts's *A Small Business Guide: Formulating A Comprehensive Written Information Security Program*[64]
- *Interagency Guidelines Establishing Information Security Standards: Small-Entity Compliance Guide*[65]
- Federal Financial Institutions Examination Council (FFIEC) *IT Examination Handbook* and *Information Security Booklet*[66]

3. Develop and Implement an Appropriate Security Program

Based on the results of the risk assessment, the law requires a business to design and implement a security program consisting of reasonable physical, technical, and administrative security measures to manage and control the risks identified during the risk assessment.[67] The security program should be

62. *See* Guin v. Brazos Higher Educ. Serv., 2006 U.S. Dist. LEXIS 4846, at *13 (D. Minn. Feb. 7, 2006) (finding that where a proper risk assessment was done, the inability to foresee and deter a specific burglary of a laptop was not a breach of a duty of reasonable care).

63. *See* NIST Spec. Publ'n No. 800-30, Rev. 1, Guide for Conducting Risk Assessments (Sept. 2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

64. *See* Mass. Office of Consumer Affairs, A Small Business Guide: Formulating A Comprehensive Written Information Security Program, http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf. *See also* Ill. Att'y Gen., Information Security and Security Breach Notification Guidance (2012), http://illinoisattorneygeneral.gov/consumers/Security_Breach_Notification_Guideance.pdf.

65. Fed. Reserve Bd. et al., Interagency Guidelines Establishing Information Security Standards: Small-Entity Compliance Guide (Dec. 14, 2005), https://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/attachment.pdf.

66. FFIEC, IT Examination Handbook InfoBase, IT Booklets, http://ithandbook.ffiec.gov/it-booklets.aspx (links to booklets).

67. *See, e.g.*, FTC, Data Security, https://www.ftc.gov/datasecurity (listing FTC data security decisions and consent decrees imposing such requirements); GLB Security Regulations (OCC), 12 C.F.R. pt. 30, app. B, pt. II.A; HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(1)(i); FISMA, 44 U.S.C. § 3544(b).

designed to provide reasonable safeguards to control the identified risks[68]—that is, to reduce them to a reasonable and appropriate level.

The presence or absence of specific security measures says little about the status of a business's legal compliance with its information security obligations. The security measures implemented by a business must respond to the particular threats it faces and address its specific vulnerabilities. Posting armed guards around a building sounds impressive as a security measure, but it is of little value if the primary threat the business faces is unauthorized remote access to its data via the Internet. Likewise, firewalls and intrusion detection software are often effective ways to stop hackers and protect sensitive databases, but if a business's major vulnerability is careless (or malicious) employees who inadvertently (or intentionally) disclose passwords or protected information, then even those sophisticated and important technical security measures will not adequately address the problem.

a. Relevant Factors to Consider

Virtually all of the existing precedent recognizes that there is no "one size fits all" approach when determining what security measures to implement within a particular business. Such a determination will depend upon a variety of factors.

Traditional negligence law suggests that the relevant factors are (1) the probability of the identified harm occurring (i.e., the likelihood that a foreseeable threat will materialize), (2) the gravity of the resulting injury if the threat does materialize, and (3) the burden of implementing adequate precautions.[69] In other words, the standard of care to be exercised in any particular case depends upon the circumstances of that case and the extent of foreseeable danger.[70]

68. *See, e.g.*, FTC, Data Security, https://www.ftc.gov/datasecurity (listing FTC data security decisions and consent decrees imposing such requirements); GLB Security Regulations, 12 C.F.R. pt. 30, app. B, pt. II.B.

69. *See, e.g.*, United States v. Carroll Towing, 159 F.2d 169, 173 (2d Cir. 1947).

70. *See, e.g.*, DCR Inc. v. Peak Alarm Co., 663 P.2d 433, 435 (Utah 1983); *see also* Glatt v. Feist, 156 N.W.2d 819, 829 (N.D. 1968) (the amount or degree of diligence necessary to constitute ordinary care varies with the facts and circumstances of each case).

Security regulations take a similar approach and indicate that the following factors are relevant in determining what security measures should be implemented:

- The probability and criticality of potential risks;
- The size, complexity, and capabilities of the business;
- The nature and scope of the business activities;
- The nature and sensitivity of the information to be protected;
- The organization's technical infrastructure, hardware, and software security capabilities;
- The state of the art of technology and security; and
- The cost of the security measures (cost was the factor mentioned most often, which suggests that businesses are not required to do everything theoretically possible).

b. Categories of Security Measures to Consider

Most laws do not require businesses to implement specific security measures or use a particular technology, but instead provide flexibility to use measures reasonably designed to achieve the objectives specified in the regulations.[71] This focus on flexibility means that, like the obligation to use "reasonable care" under tort law, determining compliance may ultimately become more difficult, as there are unlikely to be any safe harbors for security.

Nonetheless, statutes and regulations[72] consistently focus on physical, technical, and administrative security measures and, within those areas, often mention certain *categories* of security measures that businesses should consider (although how a business must address the categories is typically not specified). Those categories of security measures include the following:

- ***Physical facility and device security controls.*** Measures to safeguard the facility; measures to protect against destruction, loss, or damage of information due to potential environmental hazards (such as fire and

71. *See, e.g.*, HIPAA Security Regulations, 45 C.F.R. § 164.306(b)(1).

72. *See, e.g.*, Appendix C.2 (Federal Regulations Imposing Authentication Requirements) of this Handbook.

water damage or technological failures); procedures that govern the receipt and removal of hardware and electronic media into and out of a facility; and procedures that govern the use and security of physical workstations;

- ***Physical access controls.*** Access restrictions at buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
- ***Technical access controls.*** Software, policies, and procedures to ensure that authorized persons who need access to the system have appropriate access and that those who should not have access are prevented from getting it, including procedures to determine access authorization, grant and control access, verify that a person or entity seeking access is the one claimed (i.e., authentication), and terminate access;
- ***Intrusion detection procedures.*** Software, policies, and procedures to monitor log-in attempts and report discrepancies; system monitoring and intrusion detection systems and procedures to detect actual and attempted attacks on, or intrusions into, the organization's information systems; and procedures for preventing, detecting, and reporting malicious software (e.g., virus software);
- ***Employee procedures.*** Job control procedures, segregation of duties, and background checks for employees with responsibility for or access to protected information, and controls to prevent employees from providing information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- ***System modification procedures.*** Procedures designed to ensure that system modifications are consistent with the business's security program;
- ***Data integrity, confidentiality, and storage.*** Procedures to protect information from unauthorized access, alteration, disclosure, or destruction during storage or transmission, including storage of data in a format that cannot be meaningfully interpreted if accessed (e.g., encrypted), or in a location that is inaccessible to unauthorized persons and/or protected by a firewall;
- ***Data destruction and hardware and media disposal.*** Procedures regarding final disposition of information and/or hardware on which it resides,

and procedures for removal of data from media before reuse of the media;

- ***Audit controls.*** Maintenance of records to document repairs and modifications to the physical components of the facility related to security (walls, doors, locks, etc.), and hardware, software, and/or procedural audit control mechanisms that record and examine activity in the systems;
- ***Contingency plan.*** Procedures designed to ensure the ability to continue operations in an emergency, such as a data backup plan, disaster recovery plan, and emergency mode operation plan;
- ***Incident response plan.*** A plan for taking responsive steps if the business suspects or detects that a security breach has occurred; such steps include ensuring that appropriate persons within the organization are promptly notified of the breach, that prompt action is taken in responding to the breach (e.g., stopping further information compromise and working with law enforcement), and that persons who may be injured by the breach are appropriately notified.

4. Provide Training and Education[73]

Training and education for employees is a critical component of any security program. Even the very best physical, technical, and administrative security measures are of little value if employees do not understand their roles and responsibilities regarding security. For example, installing heavy-duty doors with state-of-the-art locks (whether physical or virtual) will not provide the intended protection if the employees authorized to have access leave the doors open or unlocked for unauthorized persons to pass through.

Security education begins with communicating applicable security policies, procedures, standards, and guidelines to employees. It also includes implementing a security awareness program, providing periodic security reminders, and developing and maintaining relevant employee training, such as user education on virus protection, password management, and how to

73. Training and education are discussed in more detail in Chapter 13 of this Handbook.

report discrepancies. It is also important to impose appropriate sanctions against employees who fail to comply with security policies and procedures.

5. Monitor and Test the Security Controls

Merely implementing security measures is not sufficient. A business also must ensure that the security measures have been properly implemented and are effective. This includes conducting an assessment of the sufficiency of the security measures in place to control the identified risks and conducting regular testing or monitoring of the effectiveness of those measures. Existing precedent also suggests that a business must monitor compliance with its security program. To that end, a regular review of records of system activity, such as audit logs, access reports, and security incident tracking reports, is also important.

6. Review and Adjust the Security Program

The legal standard for information security recognizes that security is a moving target. Law firms and other businesses must continually keep up with ever-changing threats, risks, and vulnerabilities as well as the security measures available to respond to them. This requires conducting periodic internal reviews to evaluate and adjust the information security program in light of:

- The results of the testing and monitoring;
- Any material changes to the business or client arrangements;
- Any changes in technology;
- Any changes in internal or external threats;
- Any environmental or operational changes; and
- Any other circumstances that may have a material impact.[74]

In addition to conducting periodic internal reviews, it also may be appropriate to obtain a periodic review and assessment (audit) by qualified

74. *See, e.g.*, GLB Security Regulations, 12 C.F.R. pt. 30, app. B, pt. II.E; HIPAA Security Regulations, 45 C.F.R. § 164.308(a)(8).

independent third-party professionals. Such professionals would use procedures and standards generally accepted in the profession to certify that the security program meets or exceeds applicable requirements and that the program is operating with sufficient effectiveness to provide reasonable assurances that the security, confidentiality, integrity, and availability of information are protected.

The business should then adjust the security program in light of the findings or recommendations that come from such reviews.

7. Oversee Third-Party Service Provider Arrangements

In today's business environment, companies and law firms often rely on third parties, such as outsource providers and cloud providers, to handle much of their data. When firm or client data is in the possession or under the control of a third party, this presents special security challenges. Thus, it is important to address the security of the firm's data in the possession of such third parties.

To that end, laws and regulations imposing information security obligations on businesses often expressly address requirements regarding the use of third-party outsource providers. Such rules and regulations make clear that regardless of who performs the work, the legal obligation to provide the security itself remains with the business. As it is often said, "you can outsource the work, but not the responsibility." Thus, third-party relationships should be subject to the same risk management, security, privacy, and other protection policies that would be expected if a company or firm were conducting the activities directly.[75]

Generally, the legal standard for security imposes three basic requirements on businesses that outsource: (1) they must exercise due diligence in selecting service providers, (2) they must contractually require outsource providers to implement appropriate security measures, and (3) they must monitor the performance of the outsource providers.[76]

75. *See, e.g.*, Mass. Standards for the Protection of Personal Info., 201 Mass. Code Regs. 17.02(2)(f).

76. *Id.*

G. Rules Governing Specific Data Elements and Controls

1. Special Rules for Specific Data Elements or Activities

In addition to imposing a general obligation to provide data security, some laws and regulations require protection of specific data elements, such as Social Security numbers, credit card transaction data, and other sensitive data.

The various state security breach notification laws (discussed in section III below) have created a de facto category of sensitive information in the United States. These laws require special action (i.e., disclosure) upon a breach of security for a subcategory of personal data generally considered to be sensitive because it can facilitate identity theft.

The security of Social Security numbers has been the particular focus of numerous state laws enacted in recent years.[77] The scope of these laws ranges from restrictions on the manner in which Social Security numbers can be used to requirements for security when communicating and/or storing such numbers. For example, several states have enacted laws that prohibit requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the number is encrypted.[78]

For businesses that accept credit card transactions, the PCI Standard[79] imposes significant security obligations for credit card data captured as part of any credit card transaction. The PCI Standard, jointly created by the major credit card associations, requires businesses that accept MasterCard, Visa, American Express, Discover, and Diners Club cards to comply. State law obligations also may apply.[80]

---

77. *See, e.g.*, Appendix B.5 (State SSN Laws), and Appendix B.6 (State Laws Requiring SSN Policies) of this Handbook.

78. *See* U.S. Gov't Accountability Office, GAO-05-1016T, Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain, at app. III (Sept. 15, 2005), http://www.gao.gov/assets/120/112174.pdf (list of state laws). Many federal agencies are making efforts to reduce collection, use, and display of SSNs, but have had mixed success given a number of factors (including statutes and regulations that mandate collection of SSNs); *see* U.S. Gov't Accountability Office, GAO-17-655T, Social Security Numbers: OMB and Federal Efforts to Reduce Collection, Use, and Display (May 23, 2017), https://www.gao.gov/products/GAO-17-655T.

79. *See* PCI Sec. Standards Council, Document Library, https://www.pcisecuritystandards.org/document_library.

80. *See, e.g.*, Appendix B.2 (State Laws Imposing Obligations to Provide Security for Credit Card Information) of this Handbook.

2. Duty to Encrypt Data

Some laws and regulations impose obligations to use encryption in certain situations. Initially this included state laws that mandate encryption of Social Security numbers for communication over the Internet.[81] More recently, however, some state laws prohibit the electronic transmission of any personal information to a person outside of the secure system of the business unless the information is encrypted. Most notable are the Massachusetts Regulations, which require businesses to encrypt personal information if it is stored on "laptops or other portable devices," "will travel across public networks," or will "be transmitted wirelessly."[82]

3. Duty to Destroy Data Properly

Several laws and regulations impose security requirements regarding the way that data is destroyed.[83] Such statutes and regulations generally require businesses to properly dispose of personal information by taking reasonable measures to protect against unauthorized access to, or use of, the information in connection with its disposal. For information in paper form, this typically requires implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that it cannot be read or reconstructed. For information in electronic form, such regulations typically require implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer personal information so that it cannot be read or reconstructed.

H. Frameworks for Reasonable Security

The Cybersecurity Framework is one of the deliverables contemplated by President Barack Obama's Executive Order 13,636, Improving Critical

81. *See, e.g.*, Ariz. Rev. Stat. § 44-1373; Cal. Civ. Code § 1798.85; Conn. Gen. Stat. § 42-470; Md. Code Ann., Com. Law § 14-3402(4). *See also* Appendix B.5 (State SSN Laws) of this Handbook; many state SSN laws mandate use of encryption when transmitting Social Security numbers.

82. Mass. Standards for the Protection of Personal Info., 201 Mass. Code Regs. 17.04(3) and (5).

83. *See, e.g.*, Appendix B.3 (State Data Disposal/Destruction Laws) and Appendix C.3 (Federal Data Disposal/Destruction Regulations) of this Handbook.

Infrastructure Cybersecurity, which was issued on February 12, 2013.[84] Recognizing that the national and economic security of the United States depends on the reliable functioning of the nation's critical infrastructure, the executive order directed NIST to work with the private sector to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cybersecurity risks to critical infrastructure.

Consistent with the requirements of the executive order, the Cybersecurity Framework was created through collaboration between industry and government[85] and "provides a consensus description of what's needed for a comprehensive cybersecurity program." "It reflects the efforts of a broad range of industries that see the value of and need for improving cybersecurity and lowering risk."[86] According to NIST, the Cybersecurity Framework "allows organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure."[87]

The Cybersecurity Framework references several generally accepted domestic and international security standards, and the participants generally agree that it constitutes a best practice for cybersecurity.[88] It might be argued that the Cybersecurity Framework is little more than a compilation of established industry security practices, but even so it collates such practices into a framework of activities that arguably establishes a set of requirements for the development of "reasonable" security practices. Moreover, it carries

84. Exec. Order No. 13,636, *supra* note 12.

85. The "framework is the culmination of a year-long effort that brought together thousands of individuals and organizations from industry, academia and government." Press Release, NIST, NIST Releases Cybersecurity Framework Version 1.0 (Feb. 12, 2014), https://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

86. *Id.* (quoting Under Secretary of Commerce for Standards and Technology and NIST Director Patrick D. Gallagher).

87. *Id.*

88. "Over the past year, individuals and organizations throughout the country and across the globe have provided their thoughts on the kinds of standards, best practices, and guidelines that would meaningfully improve critical infrastructure cybersecurity. The Department of Commerce's National Institute of Standards and Technology (NIST) consolidated that input into the voluntary Cybersecurity Framework that we are releasing today." Press Release, White House, Launch of the Cybersecurity Framework (Feb. 12, 2014), https://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework.

the weight of being a government-issued framework that was the result of a year-long collaboration between industry and government to develop a voluntary "how to" guide for organizations to enhance their cybersecurity.[89]

Technically, the Cybersecurity Framework was written only for businesses in the 16 critical infrastructure sectors.[90] But the practical reality goes much further. The Cybersecurity Framework is written as a generally applicable document that is in no way unique to critical infrastructure industries. It is not industry-specific, nor is it country-specific. Consistent with existing law, the Cybersecurity Framework adopts a risk-based approach to managing cybersecurity risk. As such, it appears to fit quite well with the approach of existing legal requirements for cybersecurity obligations. It provides general approaches and activities to address cybersecurity for all businesses.

"The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program."[91] The drafters of the Cybersecurity Framework contemplated that "[o]rganizations can use the framework to determine their current level of cybersecurity, set goals for cybersecurity that are in sync with their business environment, and establish a plan for improving or maintaining their cybersecurity. It also offers a methodology to protect privacy and civil liberties to help organizations incorporate those protections into a comprehensive cybersecurity program."[92]

NIST noted that "an organization without an existing cybersecurity program can use the Framework as a reference to establish one"[93] or to improve an existing program.[94]

89. *Id.*

90. According to Presidential Policy Directive 21 (PPD-21), the 16 critical infrastructure sectors are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems.

91. Cybersecurity Framework, *supra* note 46, at 13. *See generally id.* § 3.2, Establishing or Improving a Cybersecurity Program, at 13–15.

92. *See* Press Release, NIST, NIST Releases Cybersecurity Framework Version 1.0 (Feb. 12, 2014), https://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

93. Cybersecurity Framework, *supra* note 46, at 4.

94. *See id.* § 3.2.

Other cybersecurity frameworks are often used as a methodology to implement reasonable security in an organization. Two of the more commonly used are (1) the ISO/IEC 27001 framework, which was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC),[95] and (2) the Control Objectives for Information and Related Technologies (COBIT) framework, which was created by ISACA (previously known as the Information Systems Audit and Control Association).[96]

III. The Duty to Notify of Security Breaches

Legal requirements do not stop at obligations to *implement* security measures to protect data. Now there is a global trend to enact laws and regulations that impose an obligation to *disclose* security breaches to the persons affected.

A. What Is the Source of the Duty?

Today, almost all U.S. states have enacted security breach notification laws, generally based on a 2003 California law, and such obligations can also be triggered at the federal level.[97] The HIPAA regulations require breach notification,[98] as do the requirements of the federal banking regulatory agencies.[99] The IRS also has imposed a disclosure requirement with respect to taxpayers whose electronic tax records are the subject of a security breach.[100]

95. ISO/IEC 27001, Information Technology—Security Techniques—Information Security Management Systems—Requirements (2013), available for purchase at https://www.iso.org/isoiec-27001-information-security.html.

96. *See* ISACA, http://www.isaca.org/cobit/pages/default.aspx.

97. *See, e.g.*, Appendix B.4 (State Security Breach Notification Laws) and Appendix C.4 (Federal Security Breach Notification Regulations) of this Handbook.

98. 45 C.F.R. § 164.314(a)(2)(1)(C) & 45 C.F.R. § 164.410.

99. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. pt. 30, app., supp. A, pt. III (OCC), 12 C.F.R. pt. 208 (Federal Reserve System), and 12 C.F.R. pt. 364 (FDIC), and 12 C.F.R. pt. 568 (Office of Thrift Supervision, which merged with the OCC as of July 21, 2011), 70 Fed. Reg. No. 59, Mar. 29, 2005, at 15,736 [hereinafter Interagency Guidance].

100. *See* I.R.S. Rev. Proc. 98-25, § 8.01. *See* Appendix C.4 (Federal Security Breach Notification Regulations) of this Handbook.

These laws impose an obligation similar to the common law "duty to warn" of dangers, which is often based on the view that a party who has superior knowledge of a danger of injury or damage to another posed by a specific hazard must warn those who lack such knowledge. By requiring notice to persons who might be adversely affected (e.g., those whose compromised personal information may be used to facilitate identity theft), such laws seek to warn such persons that personal information has been compromised and provide an opportunity to take steps to self-protect against the consequences of identity theft.

Lawyers may have additional notification obligations under the rules of professional responsibility, other law applicable specifically to lawyers, or contractual obligations to clients.

B. What Is the Statutory Duty?

The statutory duty, as embodied in the state and federal security breach notification laws, generally requires that any business that possesses or controls certain sensitive personal information about a covered individual must disclose any breach of such information to the affected person.[101] Several statutes also require notification to the state attorney general or other regulatory agency. In some cases, notification requirements also extend to informing credit reporting agencies and the press.

The key elements of the breach notification statutes can be summarized as follows:

Type of Information. The breach notification statutes generally apply to unencrypted sensitive personally identified information—for example, information consisting of first name or initial and last name, plus one of the following: Social Security number, driver's license or state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required to access the account). In some states, this list is longer and may also include, for example, medical information, insurance policy numbers, passwords by themselves, biometric

101. Exception: Where the business maintains computerized personal information that the business does not own, the laws require the business to notify the owner or licensee of the information, rather than the individuals themselves, of any breach of the security of the system.

information, professional license or permit numbers, telecommunication access codes, mother's maiden name, employer ID number, electronic signatures, and descriptions of an individual's personal characteristics.[102]

Triggering Event. The event that triggers the obligation to provide individuals with notice of a breach involving their personal information is typically referred to in the breach statutes as a "breach of the security of the system." This term is often defined as: "unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information maintained by the person or business."[103] The requirements of this definition, in combination with certain other exclusions available in many states (e.g., an exclusion for security breaches that the custodian of the exposed data determines will not likely cause harm),[104] allow for more than one approach to determining when factors are present that impose an obligation to notify under the breach notification statutes.

Who Must Be Notified. Notice must be given to, at a minimum, any residents of the state whose unencrypted personal information was the subject of the breach. In some cases, the state's attorney general (or other enforcement agency) and/or the media must also be notified.

When Notice Must Be Provided. Generally, persons must be notified in the most expedient time possible and without unreasonable delay (although some states specify a certain number of days). In most states, the time for notice may be extended:

---

102. *See, e.g.*, Ark. Code §§ 4-110-101 *et seq.*; La. Rev. Stat. §§ 51:3071 *et seq.*; Md. Code Ann., Com. Law §§ 14-3501 *et seq.*; Neb. Rev. Stat. §§ 87-801 *et seq.*; N.J. Stat. 56:8-163; N.C. Gen. Stat. § 75-65; N.D. Cent. Code §§ 51-30-01 *et seq.*; Or. Rev. Stat. § 646A.600–.628. The Federal Banking Interagency Guidance, *see supra* note 99, also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password, or account number and password.

103. *See, e.g.*, Cal. Civ. Code § 1798.82(d).

104. For example, Iowa's Breach Notification Statute stipulates that notification is not required if "after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years." *See* Iowa Code § 715C.2(6).

- For the legitimate needs of law enforcement, if notification would impede a criminal investigation.
- To take necessary measures to determine the scope of the breach and restore reasonable integrity to the system.

Form of Notice. Notice may be provided in writing (e.g., on paper and sent by mail), in electronic form (e.g., by e-mail, but only in compliance with E-SIGN[105]), or by substitute notice. If the cost of providing individual notice is greater than a certain amount (e.g., $250,000), or if more than a certain number of people would have to be notified (e.g., 500,000), the business may use substitute notice, consisting of:

- E-mail, when the e-mail address is available, and
- Conspicuous posting on the entity's website, and
- Publishing notice in all major statewide media.

Requirements vary from state to state, however, and some requirements have become controversial. One of the biggest issues concerns the nature of the triggering event. In California, for example, notification is required whenever there has been unauthorized access that compromises the security, confidentiality, or integrity of electronic personal data. In other states, unauthorized access does not trigger the notification requirement unless there is a reasonable likelihood of harm to the individuals whose personal information is involved or unless the breach is material.

C. When Does a Contract-Based Duty Arise?

It is increasingly common for contracts with business partners of all types to require the recipient or processor of a business's data to notify that party in the event of a breach. This trend is also being extended to law firms. Clients (particularly in regulated industries such as financial or healthcare) are requiring that their law firms provide prompt notice of any security breach. For example, breach reporting is a key requirement of the Model

105. 15 U.S.C. §§ 7001 *et seq.* This generally requires that entities comply with the requisite consumer consent provisions of E-SIGN at 15 U.S.C. § 7001(c).

Information Protection and Security Controls for Outside Counsel Processing Company Confidential Information, released in 2017 by the Association of Corporate Counsel.[106]

IV. Practical Considerations: A Top Ten List

Lawyers have many legal obligations to provide data security. Below is a list of practical tips regarding compliance with those obligations:

1. Identify the data you have (yours, your clients', data obtained during due diligence or discovery) and understand where it is stored, how it can be accessed, and how it is used.
2. Evaluate the risks to the data you have.
3. Develop a written security program to protect that data against the identified risks.
4. If you use third parties (e.g., providers of cloud services or outsourcing services) to store or process the data, take appropriate steps to make sure that they adequately protect the security of the data you entrust to them.
5. On a regular basis, reevaluate the risks you face and the adequacy of your security program, and adjust the program as necessary.
6. Determine which data (yours, your clients', data obtained during due diligence or discovery) is subject to which laws and regulations (including special sector-specific regulations such as GLB or HIPAA), and be sure you handle it in accordance with any special requirements in those laws and regulations.
7. Recognize that other lawyers and staff within the firm can be a weak link, and provide appropriate training and awareness-raising reminders for all lawyers and staff.

106. Ass'n of Corporate Counsel, Model Information Protection and Security Controls for Outside Counsel Processing Company Confidential Information (Jan. 2017), http://www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf.

8. Develop an incident response plan that covers the data you have.
9. Keep in mind that laws and regulations governing data security may apply to all of the data in your possession, independent of ethical obligations specifically applicable to attorneys.
10. Remember that security is a process and is never complete, so you must remain vigilant for new threats.

NOTES

19

New York Attorney General, Press Release: A.G. Schneiderman Announces $575,000 Settlement With EmblemHealth After Data Breach Exposed Over 80,000 Social Security Numbers (March 6, 2018)

Submitted by:
Clark Russell

New York State Office of the Attorney General

Español

A.G. Schneiderman Announces $575,000 Settlement With EmblemHealth After Data Breach Exposed Over 80,000 Social Security Numbers

News from Attorney General Eric T. Schneiderman

FOR IMMEDIATE RELEASE
March 6, 2018

Attorney General's Press Office / 212-416-8060
nyag.pressoffice@ag.ny.gov
Twitter: @AGSchneiderman

EmblemHealth Agrees to Implement Corrective Action Plan and Conduct Comprehensive Risk Assessment

AG Schneiderman Renews Call to Pass SHIELD Act to Protect New Yorkers From Data Breaches

NEW YORK – Attorney General Eric T. Schneiderman today announced a settlement with healthcare provider EmblemHealth and wholly owned subsidiary Group Health Incorporated ("EmblemHealth") after the company admitted a mailing error that resulted in 81,122 social security numbers being disclosed on a mailing. In addition to paying a $575,000 penalty, EmblemHealth agreed to implement a Corrective Action Plan and conduct a comprehensive risk assessment.

Attorney General Schneiderman today reiterated his call to improve New York's weak and outdated security laws with the **"Stop Hacks and Improve Electronic Data Security Act" (or "SHIELD Act")**. Introduced by the Attorney General in November 2017, the SHIELD Act would comprehensively protect New Yorkers' personal information from the growing number of data breaches and close major gaps in New York's data security laws, without putting an undue burden on businesses.

"The careless handling of social security numbers is never acceptable," said **Attorney General Schneiderman**. "New Yorkers need to be able to trust that companies entrusted with their private information will guard it appropriately. This starts with good governance—

which is why my office will continue to push for stronger security laws and hold businesses accountable for protecting their customers' personal data."

EmblemHealth is one of the largest health plans in the United States. On October 13, 2016, it discovered that it had mailed 81,122 policyholders, including 55,664 New York residents, a paper copy of their Medicare Prescription Drug Plan Evidence of Coverage ("EOC Mailing") that included a mailing label with the policyholder's social security number on it. Normally, all mailings include a unique mailing identifier that is printed on the envelope. However, in this case, the mailing inadvertently included the insured's Health Insurance Claim Number, which incorporated the insured's social security number.

Pursuant to the federal Health Insurance Portability Accountability Act, as amended by the Health Information Technology for Economic and Clinical Health Act ("HIPAA"), EmblemHealth is required to safeguard patients' protected health information, including social security numbers, and utilize appropriate administrative, physical and technical safeguards. In connection with its 2016 EOC Mailing, EmblemHealth failed to comply with many of the standards and procedural specifications as required by HIPAA. Printing an individual's social security number on "a postcard or other mailer not requiring an envelope, or visible on the envelope, or without the envelope having been opened" also violates New York General Business Law § 399-ddd(2)(e).

In addition to paying a $575,000 penalty, under the settlement EmblemHealth must implement a Corrective Action Plan that includes a thorough risk analysis of security risks associated with the mailing of policy documents to policyholders, and submit a report of those findings to the Attorney General's office within 180 days of the settlement. EmblemHealth must also review and revise its policies and procedures based on the results of the assessment, and notify the Attorney General's office of any action it takes. If no action is taken, EmblemHealth must provide a written detailed explanation of why no action is necessary. EmblemHealth must also catalogue, review, and monitor mailings and make reasonable efforts to ensure: (a) all relevant workforce members are adequately trained for each discrete job function that they are tasked with or assigned to perform related to mailings; (b) report any known violations of EmblemHealth policies and procedures relating to the HIPAA Minimum Necessary Standard, as set forth in 45 C.F .R. § 164.502(b) and § 164.514(b), to the appropriate EmblemHealth official and remediate any known violations as soon as practicable; and (c) for a period of three (3) years, report security incidents involving the loss or compromise of New York residents' information to the Attorney General's office that might not otherwise trigger the reporting requirements of New York State law.

This case was handled by Bureau of Internet and Technology Deputy Bureau Chief Clark Russell, under the supervision of Bureau Chief Kathleen McGee. The Bureau of Internet and Technology is overseen by Executive Deputy Attorney General for Economic Justice Manisha M. Sheth.

Attorney General's Press Office: (212) 416-8060

nyag.pressoffice@ag.ny.gov

Press Release Archive

- February 2019
- January 2019
- December 2018
- November 2018
- October 2018
- September 2018
- August 2018
- July 2018
- June 2018
- May 2018
- April 2018
- March 2018

VIEW ALL PRESS RELEASE ARCHIVES

Search:

Search

NOTES

20

New York Attorney General, Press Release: A.G. Underwood Announces Record $148 Million Settlement With Uber Over 2016 Data Breach (September 26, 2018)

Submitted by:
Clark Russell

New York State Office of the Attorney General

Español

A.G. Underwood Announces Record $148 Million Settlement With Uber Over 2016 Data Breach

News from the New York Attorney General's Office

FOR IMMEDIATE RELEASE
September 26, 2018

Attorney General's Office Press Office / 212-416-8060
nyag.pressoffice@ag.ny.gov

A.G. UNDERWOOD ANNOUNCES RECORD $148 MILLION SETTLEMENT WITH UBER OVER 2016 DATA BREACH

Settlement with 50 States & DC Also Requires Uber to Adopt Model Data Breach Notification and Data Security Practices, Corporate Integrity Program; Hire Independent Third Party to Assess Data Security

NEW YORK – Attorney General Barbara D. Underwood today announced an agreement with ride-sharing company Uber Technologies, Inc. (Uber) to settle allegations it intentionally concealed a 2016 data breach in violation of state data breach notification laws. The settlement, which was reached with all 50 states and the District of Columbia, requires Uber to adopt model data breach notification and data security practices and a corporate integrity program for employees to report unethical behavior, and hire an independent third party to assess its data security practices. It also requires Uber to pay a record penalty of $148 million.

"New Yorkers deserve to know that their personal information will be protected – period," said **Attorney General Underwood.** "This record settlement should send a clear message: we have zero tolerance for those who skirt the law and leave consumer and employee information vulnerable to exploitation. We'll continue to fight to protect New Yorkers from weak data security and criminal hackers."

In November 2016, hackers based in the United States and Canada secretly informed security officials at Uber that they had downloaded the personal information of 57 million riders and drivers, 25 million of whom were in the United States and 7.7 million of whom were drivers. The information stolen included names, email addresses, and mobile phone numbers;

drivers' license information pertaining to approximately 600,000 drivers nationwide was also stolen. After providing proof of the massive data breach, the hackers demanded "six figures" to delete the data and not disclose the breach. Uber ultimately paid the hackers $100,000 to conceal the breach.

In the spring of 2017, Uber's Board of Directors directed a law firm to investigate Uber's security team in the wake of unrelated litigation involving the alleged theft of trade secrets related to self-driving cars. As part of this inquiry, the law firm learned of the breach and ransom payment. Upon learning of the breach, the board hired a forensic firm to investigate the breach. Uber ultimately provided notice of the breach in late November 2017, a year after the breach.

General Business Law § 899-aa requires companies that experience a breach involving certain personal information, including driver's license numbers, to provide notice "in the most expedient time possible and without unreasonable delay." By intentionally concealing the breach and failing to disclose it for a year, Uber violated GBL § 899-aa.

As part of the nationwide settlement, Uber has agreed to pay a record penalty of $148 million to the states. New York will receive approximately $5.1 million.

The settlement between New York and Uber requires the company to:

- Comply with New York's data breach and consumer protection laws regarding protecting New York residents' personal information and notifying them in the event of a data breach concerning their personal information;
- Take precautions to protect any user data Uber stores on third-party platforms outside of Uber;
- Use strong password policies for its employees to gain access to the Uber network;
- Develop and implement a strong overall data security policy for all data that Uber collects about its users, including assessing potential risks to the security of the data and implementing any additional security measures beyond what Uber is doing to protect the data;
- Hire an outside qualified party to assess Uber's data security efforts on a regular basis and draft a report with any recommended security improvements. Uber will implement any such security improvement recommendations; and

- Develop and implement a corporate integrity program to ensure that Uber employees can report any ethics concerns they have about any other Uber employees to the company.

This settlement also addresses and resolves allegations that Uber's conduct violated an earlier 2016 settlement with the Office of the New York Attorney General. In the earlier investigation, the office found that on May 12, 2014, a hacker accessed an Uber database that included names of roughly 50,000 Uber drivers and their driver's license numbers. Uber discovered the breach in September 2014 but did not provide notice to the affected drivers and the office until February 26, 2015, over five months later. The prior 2016 settlement required Uber to comply with GBL § 899-aa. It also required Uber to adopt protective technologies for the storage, access, and transfer of certain personal information, and credentials related to its access, including the adoption of multi-factor authentication, or similarly protective access control methodologies.

The New York Attorney General independently investigated the current breach, but later joined the multistate investigatory process, where it took a leadership position, to effectuate settlement.

The Attorney General's office has also **proposed legislation to close gaps in New York's data security laws** and comprehensively protect New Yorkers' personal information from data breaches.

The case was handled by Bureau of Internet and Technology Deputy Bureau Chief Clark Russell, under the supervision of Bureau Chief Kim A. Berger. The Bureau of Internet and Technology is overseen by Executive Deputy Attorney General for Economic Justice Manisha M. Sheth.

Attorney General's Press Office: (212) 416-8060

nyag.pressoffice@ag.ny.gov

Press Release Archive

- February 2019
- January 2019
- December 2018

- November 2018
- October 2018
- September 2018
- August 2018
- July 2018
- June 2018
- May 2018
- April 2018
- March 2018

VIEW ALL PRESS RELEASE ARCHIVES

Search:

Search

NOTES

NOTES

21

New York Attorney General, Press Release: A.G Underwood Announces Record COPPA Settlement With Oath – Formerly AOL – For Violating Children's Privacy (December 4, 2018)

Submitted by:
Clark Russell

New York State Office of the Attorney General

Español

A.G. Underwood Announces Record COPPA Settlement With Oath – Formerly AOL – For Violating Children's Privacy

News from the New York Attorney General's Office

FOR IMMEDIATE RELEASE
December 4, 2018

Attorney General's Office Press Office / 212-416-8060
nyag.pressoffice@ag.ny.gov

A.G. UNDERWOOD ANNOUNCES RECORD COPPA SETTLEMENT WITH OATH – FORMERLY AOL – FOR VIOLATING CHILDREN'S PRIVACY

Company Conducted Billions of Auctions for Targeted Ads on Hundreds of Children's Websites in Violation of COPPA

Company Agrees To Pay $4.95 Million – the Largest Penalty Ever in a COPPA Enforcement Matter in U.S. History – and Adopt Comprehensive Reforms to Protect Children from Improper Tracking

NEW YORK – Attorney General Barbara D. Underwood today announced a record settlement with Oath, Inc., formerly known as AOL, for violating the Children's Online Privacy Protection Act (COPPA), marking the largest-ever penalty in a COPPA enforcement matter in U.S. history.

The Attorney General's Office found that AOL conducted billions of auctions for ad space on hundreds of websites the company knew were directed to children under the age of 13. Through these auctions, AOL collected, used, and disclosed personal information from the websites' users in violation of COPPA, enabling advertisers to track and serve targeted ads to young children. The company has agreed to adopt comprehensive reforms to protect children from improper tracking and pay a record $4.95 million in penalties, the largest penalty ever in a COPPA enforcement matter in U.S. history.

Oath Inc. is a wholly-owned subsidiary of Verizon Communications Inc. Until June 2017, Oath was known as AOL Inc. ("AOL").

"COPPA is meant to protect young children from being tracked and targeted by advertisers online. AOL flagrantly violated the law – and children's privacy – and will now pay the largest-ever penalty under COPPA," said **Attorney General Barbara Underwood**. "My office remains committed to protecting children online and will continue to hold accountable those who violate the law."

The Children's Online Privacy Protection Act

In 1998, Congress enacted COPPA to protect the safety and privacy of young children online. COPPA prohibits operators of certain websites from collecting, using, or disclosing personal information (e.g., first and last name, e-mail address) of children under the age of 13 without first obtaining parental consent. Operators of websites and online services directed to children under the age of 13, and the operators of websites and online services that have actual knowledge that they are collecting personal information from a child under the age of 13, are subject to COPPA.

In July 2013, the definition of "personal information" was revised to include persistent identifiers that can be used to recognize a user over time and across websites, such as the ID found in a web browser cookie or an Internet Protocol ("IP") address. The revision effectively prohibits covered operators from using cookies, IP addresses, and other persistent identifiers to track users across websites for most advertising purposes, amassing profiles on individual users, and serving online behavioral advertisements on COPPA-covered websites.

How Targeted Advertising Works

Most online shoppers have encountered advertisements for a product that seems to follow them from website to website. These advertisements are known as online behavioral advertisements or OBA, a form of targeted advertising that selects an advertisement to serve to an individual based on previously collected information about that individual, such as the individual's Internet browsing history, demographic information, or personal interests.

OBA ads are often placed through online marketplaces known as ad exchanges. An ad exchange enables websites to sell, and advertisers to buy, advertising space through an auction process. Auctions take place in real-time, after a user opens a webpage that contains ad space.

When a user opens a webpage on a site that works with an ad exchange, the exchange retrieves a small text file stored on the user's computer known as a web browser cookie. The exchange typically transmits information from that cookie to entities that may be interested in purchasing ad space on behalf of advertisers. These

entities use the information the exchange provides to help determine whether to place a bid for the ad space on behalf of an advertiser. The exchange collects bids, selects a winner, and then permits the winning bidder to serve an advertisement, usually an OBA ad, to the user. The entire auction process takes place in a fraction of a second.

AOL's Display Ad Exchange Conducted Billions of Auctions in Violation of COPPA

AOL operates several ad exchanges, including an exchange for image-based ads, referred to as "display" ads. Until recently, AOL's ad exchange for display ads was not capable of conducting a COPPA-compliant auction that involved third-party bidders because AOL's systems would necessarily collect information from users and disclose that information to the third-parties. AOL policies therefore prohibited the use of its display ad exchange to auction ad space on COPPA-covered websites to third-parties.

Despite these policies, AOL nevertheless used its display ad exchange to conduct billions of auctions for ad space on websites that it *knew* to be directed to children under the age of 13 and subject to COPPA.

AOL obtained this knowledge in two ways. First, several AOL clients provided notice to AOL that their websites were subject to COPPA. These clients identified more than a dozen COPPA-covered websites to AOL. AOL conducted at least 1.3 billion auctions of display ad space from these websites.

Second, AOL itself determined that certain websites were directed to children under the age of 13 when it conducted a review of the content and privacy policies of client websites. Through these reviews, AOL identified hundreds of additional websites that were subject to COPPA. AOL conducted at least 750 million auctions of display ad space from these websites.

AOL Placed Ads Through Other Exchanges in Violation of COPPA

AOL also operates a business that bids on ad space in auctions conducted by other ad exchanges. Several of the exchanges that AOL has worked with have the capability to auction ad space on child-directed websites in a COPPA-compliant manner. When one of these exchanges conducts an auction for ad space on a child-directed website, the exchange passes information to bidders indicating that it is subject to COPPA. Bidders that receive this information are expected to comply with COPPA as well.

Prior to November 2017, AOL's systems ignored any information that it received from an ad exchange indicating that the ad space was subject to COPPA. Thus, whenever AOL participated

in and won an auction for COPPA-covered ad space, its systems behaved as they normally did. In these cases, the company typically used user information supplied by the exchange and information the company could collect directly from the user to select and serve a targeted advertisement to the user. AOL's collection and use of this information from users on COPPA-covered websites violated COPPA.

An AOL Account Manager Knowingly Violated COPPA to Increase Revenue

As described above, AOL permitted clients to use its display ad exchange to sell ad space on COPPA-covered sites, even though the exchange was not capable of conducting a COPPA-compliant auction that involved third-party bidders. AOL documents show that an AOL account manager based in New York intentionally configured at least one of these client's accounts in a manner that she *knew* would violate COPPA in order to increase advertising revenue. In addition, AOL documents show that the NY account manager repeatedly represented to at least this client that AOL's display ad exchange *could* be used to sell ad space to third-parties in a COPPA compliant manner. As a result of these misstatements, the client used AOL's display ad exchange to place more than a billion advertisements on COPPA-covered inventory.

Company Must Adopt Comprehensive Reforms to Protect Kids Privacy

AOL has agreed to adopt comprehensive reforms to its policies and procedures to protect children's privacy. The agreement requires that AOL establish and maintain a comprehensive COPPA compliance program that includes: the designation of an executive or officer to oversee the program; annual COPPA training for relevant AOL personnel; the identification of risks that could result in AOL's violation of COPPA; the design and implementation of reasonable controls to address the identified risks, as well as regular monitoring of the effectiveness of those controls; and development and use of reasonable steps to select and retain service providers that can comply with COPPA. The agreement also requires that AOL retain an objective, third-party professional to assess the privacy controls that the company has implemented.

In addition, AOL has agreed to implement and maintain functionality that enables website operators that sell ad inventory through AOL systems to indicate each website or portion of a website that is subject to COPPA. AOL will maintain this information in a database or similar system, and disclose to each third-party bidder that relevant ad space is subject to COPPA.

Finally, AOL has also agreed to destroy all personal information collected from children that is in its possession, custody, or control, unless such personal information is required to be maintained by law, regulation, or court order.

Operation Child Tracker

Today's announcement builds on the Attorney General's office's prior work protecting children's privacy through Operation Child Tracker, an ongoing investigation into illegal tracking of children's online activity by marketers, advertising companies, and others in violation of COPPA. In September 2016, the **Attorney General's office announcedsettlements with four companies that had violated COPPA** by allowing illegal third-party tracking technologies on some of the nation's most popular kids' websites, including websites for Barbie, Nick Jr., My Little Pony, American Girl, Hot Wheels, and dozens of others. Those companies agreed to pay penalties totaling $835,000 and to adopt comprehensive reforms to protect children from improper tracking and the collection of children's personal information in the future. Then in April 2017, the **Attorney General's office announced a settlement with the operator of a COPPA safe harbor program** for flawed privacy assessments that left children visiting popular children's websites vulnerable to illegal tracking. As part of that settlement, the company paid a penalty of $100,000 and agreed to adopt new measures to strengthen its privacy assessments.

This case was handled by Bureau of Internet and Technology Assistant Attorney General Jordan Adler and Deputy Bureau Chief Clark Russell, under the supervision of Bureau Chief Kim Berger. The Bureau of Internet and Technology is overseen by Executive Deputy Attorney General for Economic Justice Manisha M. Sheth.

Attorney General's Press Office: (212) 416-8060

nyag.pressoffice@ag.ny.gov

Press Release Archive

- February 2019
- January 2019
- December 2018
- November 2018

- October 2018
- September 2018
- August 2018
- July 2018
- June 2018
- May 2018
- April 2018
- March 2018

VIEW ALL PRESS RELEASE ARCHIVES

Search:

Search

NOTES

NOTES

22

New York Attorney General, Press Release: A.G Underwood Announces Settlements with Five Companies Whose Mobile Apps Failed to Secure User Information Transmitted Over the Internet (December 14, 2018)

Submitted by:
Clark Russell

New York State Office of the Attorney General

A.G. Underwood Announces Settlements With Five Companies Whose Mobile Apps Failed To Secure User Information Transmitted Over The Internet

News from the New York Attorney General's Office

FOR IMMEDIATE RELEASE
December 14, 2018

Attorney General's Office Press Office / 212-416-8060
nyag.pressoffice@ag.ny.gov

A.G. UNDERWOOD ANNOUNCES SETTLEMENTS WITH FIVE COMPANIES WHOSE MOBILE APPS FAILED TO SECURE USER INFORMATION TRANSMITTED OVER THE INTERNET

Mobile Apps Operated by Western Union, Priceline, Equifax, Spark Networks, and Credit Sesame Suffered from Well-Known Security Vulnerability

Companies Have Agreed to Implement Comprehensive Security Program to Protect App Users' Information

Part of AG Initiative to Uncover Critical Security Vulnerabilities Before User Info is Stolen

NEW YORK – Attorney General Barbara D. Underwood today announced settlements with five companies – Western Union Financial Services, Inc. ("Western Union"), Priceline.com, LLC ("Priceline"), Equifax Consumer Services, LLC ("Equifax"), Spark Networks, Inc. ("Spark Networks"), and Credit Sesame, Inc. ("Credit Sesame") – for having mobile apps that failed to keep sensitive user information secure when transmitted over the Internet. The companies' mobile apps suffered from a well-known security vulnerability that could have allowed sensitive information entered by users – such as passwords, social security numbers, credit card numbers, and bank account numbers – to be intercepted by eavesdroppers employing simple and well-publicized techniques. Although each company represented to users that it used reasonable security measures to protect their information, the companies failed to

sufficiently test whether their mobile apps had this vulnerability. Today's settlements require each company to implement comprehensive security programs to protect user information.

"Businesses that make security promises to their users – especially as it relates to personal information – have a duty to keep those promises," said **Attorney General Underwood**. "My office is committed to holding businesses accountable and ensure they protect users' personal information from hackers."

The settlements announced today are the result of an initiative undertaken by the Attorney General's office to uncover critical security vulnerabilities *before* user information is stolen. As part of this initiative, the office tested dozens of mobile apps that handle sensitive user information, such as credit card and bank account numbers.

Establishing a Secure Connection Using TLS

Consumers in public places, such as coffee shops and airports, frequently use WiFi networks to connect their mobile phones and tablets to the Internet. In these settings, public WiFi provides an opportunity for eavesdroppers to intercept, and even modify, the data that mobile devices send and receive. To protect this data, mobile web browsers and apps use a security protocol known as Transport Layer Security (TLS) to establish a secure, encrypted connection over the Internet.

To establish a secure TLS connection between a mobile device and another computer, the mobile device must verify the computer's identity. It does so using credentials the computer provides through a file known as an SSL/TLS certificate.

An app that fails to properly authenticate a certificate is vulnerable to a "man-in-the-middle attack." This is a method of eavesdropping that allows someone positioned between the mobile device and computer ("in-the-middle") to intercept and view any information that the mobile device and computer transmit to each other, even if that information has been encrypted. A man-in-the-middle attack can be performed using a WiFi-enabled laptop and freely available software and can be virtually undetectable by the user of the mobile device.

This vulnerability has been well-known in the industry for many years. For example, in 2014, several teams of security researchers independently announced that they had identified apps that suffered from the vulnerability. In addition, in March 2014, the Federal Trade Commission announced that the maker of two apps had agreed to settle charges relating to their apps' failure to properly validate SSL certificates.

App developers can test their mobile apps for this vulnerability using freely available software.

The Companies' Flawed Implementation of TLS

Western Union, Priceline, Equifax, Spark Networks, and Credit Sesame offered free mobile apps for download through Apple's "App Store" and Google's "Play Store." Users of these apps were required to enter information into the apps, such as log-in credentials (e.g. email address and password) to create or access a user account, and credit card numbers to make purchases.

Certain versions of the companies' apps all failed to properly authenticate the SSL/TLS certificates they received. As a result, an attacker could have impersonated the companies' servers and intercepted information entered into the app by the user. With this information, an attacker could commit various forms of identity theft and fraud, including credit card fraud. Pursuant to their settlement agreements, each company will implement comprehensive security programs to protect user information from future potential attacks.

This case was handled by Assistant Attorneys General Jordan Adler and Johanna Skrzypczyk and Deputy Director of Strategic Initiatives Vanessa Ip, under the supervision of Bureau Chief Kim A. Berger and Deputy Bureau Chief Clark P. Russell, all of the Bureau of Internet and Technology. The Bureau of Internet and Technology is overseen by Executive Deputy Attorney General for Economic Justice Manisha M. Sheth.

Attorney General's Press Office: (212) 416-8060

nyag.pressoffice@ag.ny.gov

Press Release Archive

- February 2019
- January 2019
- December 2018
- November 2018
- October 2018
- September 2018
- August 2018
- July 2018

- June 2018
- May 2018
- April 2018
- March 2018

VIEW ALL PRESS RELEASE ARCHIVES

NOTES

NOTES

23

Discoverability of Witness Interviews in California: Application of the Work Product Doctrine and the Attorney-Client Privilege

Merri A. Baldwin

Rogers Joseph O'Donnell

Discoverability of Witness Interviews in California: Application of the Work Product Doctrine and the Attorney-Client Privilege

By: Merri A. Baldwin

Attorneys often conduct witness interviews as part of an investigation, whether as witnesses to an accident, corporate employees as part of an investigation, or co-defendants who are part of a multi-party lawsuit. Lawyers may conduct the interviews themselves or use non-lawyer personnel such as legal assistants or investigators to assist. Counsel may record the interview, take notes, draft a summary, or report in an email the information the witness provided. In California, the attorney-client privilege and/or attorney work product doctrine provide varying levels of protection against disclosure, depending upon the factors including the content of the writing memorializing the interview and the circumstances of the interview itself. Whether seeking to obtain such documents in discovery, or to protect them from discovery, it is important for attorneys to understand the law in this area.

Attorney-Client Privilege and Work-Product Doctrine

Both the attorney-client privilege and the attorney work-product doctrine provide protection from disclosure to third parties of certain materials created as part of an attorney-client relationship. An attorney owes clients the duty to "maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets" of the clients. (Bus. & Prof. Code §6068(e); *see also* California Rule of Professional Conduct 3-100).

The attorney-client privilege is an evidentiary rule that protects from disclosure to third parties communications from an attorney to a client. (*See* Cal. Evidence Code section 954) Its fundamental purpose is to "safeguard the confidential relationship between clients and their attorneys so as to promote full and open discussion of the facts and tactics surrounding individual legal matters." *Gordon v. Superior Court*, 55 Cal. App. 4th 1546, 1557 (1997)(citations omitted).

The work product doctrine is set forth in section 2018.030 of the Code of Civil Procedure. Its purpose is to allow attorneys to "prepare cases for trial with that degree of privacy necessary to encourage them to prepare their cases thoroughly and to investigate not only the favorable but the unfavorable aspects of their cases," (2018.020(a)), and to "[p]revent attorneys from taking undue advantage of their adversary's industry and efforts." Sect. (2018.020(b)). The statute provides absolute protection to any "writing that reflects an attorney's impressions, conclusions, opinions, or legal research or theories." Sect. 2018.030(a). Such a writing is not discoverable under any circumstances. *Id.* Other work product has more qualified protection in that it is "not discoverable unless the court determines that denial of discovery will unfairly prejudice the party seeking discovery in preparing that party's claim or defense or will result in an injustice." Sect. 2018.030(b).

The statute does not define "work product." Courts have considered the issue on a case by case basis and have generally concluded that only "derivative" or "interpretive" material, that is, "material created by or derived from an attorney's work reflecting the attorney's evaluation of the law or facts," qualifies as work product. *See Coito v. Superior Court*, 54 Cal. 4th 480, 488

(2012). Nonderivative material, such as "the identity and location of physical evidence or witnesses," does not constitute work product. *Id*. at 489.

Recorded Witness Statements as Work Product

Prior to the California Supreme Court's decision in *Coito v. Superior Court*, 54 Cal. 4th 480 (2012), the question of whether recorded witness statements obtained by investigators were protected against disclosure on work product grounds was unsettled. The Court in *Rico v. Mitsubishi Motors Corp.*, 42 Cal. 4th 807 (2007) had held that attorney notes or summaries of witness interviews were protected as work product, but the Court had not previously examined the issue of whether section 2018.030 applied to witness statements.

In *Coito*, the California Supreme Court clarified the reach of the attorney work product doctrine. The case arose after an accident that resulted in the drowning death of a 13-year-old boy. The child's mother filed a complaint for wrongful death against the State of California, among other parties. The Attorney General's office sent two investigators to conduct audio-recorded interviews of four of the six witnesses to the accident. In discovery, the plaintiff sought production of the audio recordings. The state asserted the work product privilege, relying on the Third District's ruling in *Nacht & Lewis Architects, Inc. v. Superior* Court, 47 Cal. App. 4th 214 (1996), which held that the absolute work privilege applies to witness statements recorded by an attorney. The trial court relied on *Nacht* and largely denied the motion to compel. The Court of Appeal, criticizing *Nacht* and relying on *Greyhound Corporation v. Superior Court*, 57 Cal. 2d 355 (1961), concluded that witness statements are not entitled to work product protection as a matter of law.

The Supreme Court reversed the Court of Appeal to hold that witness statements obtained through an attorney-directed interview are entitled to work product protection. "In light of the origins and development of the work product privilege in California, we conclude that witness statements obtained as a result of an interview conducted by an attorney, or by an attorney's agent at the attorney's behest, constitute work product protected by section 2018.030." 54 Cal. 4th at 494.

The Court held that where a witness statement reveals an attorney's impressions, conclusions, opinions, or legal research, the statement is entitled to absolute protection. This would include witness statements "inextricably intertwined" with the attorney's notes or comments, or where the questions asked (or not asked) "provide a window" into the attorney's theory of the case or evaluation of the issues. 54 Cal. 4th at 495. The Court went on to hold that where witness statements obtained by an attorney do not reveal the attorney's thought processes (and therefore would not constitute absolute work product), those are nevertheless entitled as a matter of law to qualified work product protection, since production of these statements would undermine the legislative policy of preventing an attorney from taking advantage of an adversary's efforts. "Even when an attorney who exercises no selectivity in determining which witnesses to interview, . . . the attorney has expended time and effort in identifying and locating each witness, securing the witness' willingness to talk, listening to what the witness said, and preserving the witness' statement for possible future use." 54 Cal. 4th at 496. Statements that would qualify for the lower level of protection would include, the Court stated, those obtained by "an attorney with no particular foresight, strategy, selectivity, or planning." *Id.*

Under *Coito*, a party objecting to producing recorded statements on the grounds they are entitled to absolute protection must make a preliminary or foundational showing that disclosure would reveal the attorney's "impressions, conclusions, opinions, or legal research or theories." Upon adequate showing, the trial court would then determine (including through an *in camera* inspection if necessary) whether and to what extent the absolute privilege applies, thereby potentially shielding all or portions of recorded interviews from discovery.

Certain factors will increase the likelihood that witness interviews and statements will be entitled to absolute work product protection, according to the Court. These include: explicit comments or notes by the attorney stating his or her impressions of the witness or other case issues; questions asked of the witness that provide insight into the attorney's theory of the case or evaluation of what issues are most important; and follow-up questions that potentially reveal the attorney's strategy or concerns. ("Lines of inquiry that an attorney chooses to pursue through follow-up questions may be especially revealing.") In addition, the very identity of particular witnesses interviewed could reveal an attorney's thoughts or evaluation. 54 Cal. 4th at 496. Under certain circumstances, the Court stated, it may be possible to redact a witness statement and thereby protect absolute work product. *Id.* In other instances, redactions will not offer sufficient protection and the statement will be protected from disclosure. For example, the witness' statements may themselves reveal the questions asked. *Id.*

To the extent the absolute privilege does not apply, parties seeking production of recorded witness statements or interviews will have the burden on a motion to compel of showing that "denial of disclosure will unfairly prejudice the party in preparing its claims or will result in an injustice." 54 Cal. 4th at 500. After *Coito*, any party seeking recorded witness statements in discovery should anticipate filing a motion to compel, and, if it can be shown that the material is entitled only to qualified protection, be prepared to show that denial of disclosure will unfairly prejudice the party in preparing its claim or defense or will result in an injustice.[1]

Protection Available to Employee Statements Provided During A Confidential Attorney Investigation

While the issue in *Coito* concerned witness statements obtained in litigation, a different but equally important question concerns the protection available to statements by corporate employees obtained by an attorney during the course of a confidential investigation on behalf of the corporate client. The California Supreme Court in *Costco Wholesale Corporation v. Superior Court*, 47 Cal. 4th 725 (2009) held that an attorney's written opinion letter following a confidential investigation is privileged, but did not reach the issue of whether witness statements obtained during that investigation would be protected against later discovery.

Attorneys are often called upon to conduct investigations on behalf of their clients. Some investigations are conducted for the purpose of assisting a client with legal advice, and are

[1] *Coito* also concerned the issue of whether information responsive to form interrogatory 12.3 is protected as work product. That interrogatory seeks the identity of any witness from whom the attorney has obtained a written or recorded statement. The Court held that in certain cases, such information may be protected. 54 Cal. 4th at 502.

intended to remain confidential. Others are conducted with the expectation that the results will be disclosed. Witness interviews are an important part of most if not all investigations.

In *Costco*, the retail company retained a law firm to provide legal advice as to whether certain employees were exempt under California wage and overtime law. The law firm conducted an investigation, which included interviews by an attorney of Costco employees. Costco, the lawyer, and the two employees understood that the interviews were confidential and would remain so. 47 Cal. 4th at 730. The lawyer ultimately produced a 22-page opinion letter for the client.

Several years later, Costco employees filed a class action against Costco and sought production of the opinion letter. Costco objected on grounds of privilege and work product. The trial court ordered an *in camera* review of the report by a discovery referee. The referee redacted the opinion letter to excise the portions that contained "attorney observations, impressions and opinions," leaving factual information about various employees' job responsibilities, and recommended its production. 47 Cal. 4th at 731. The basis for the referee's decision was that "statements obtained in attorney interviews of corporate employee witnesses generally are not protected by the corporation's attorney-client privilege and do not become cloaked with the privilege by reason of having been communicated between the attorney and the client." *Id.* The trial court ordered Costco to produce the redacted letter. Costco petitioned for a writ of mandate, and the Court of Appeal denied the petition.

The Supreme Court held that "the attorney-client privilege attaches to [the] opinion letter in its entirety, irrespective of the letter's content." 47 Cal. 4th at 732. The Court held that the facts supported a prima facie case of privilege: a corporation may claim the privilege (Evid. Code section 954); the corporation retained the lawyer for the purpose of seeking legal advice; and the letter was confidential. 47 Cal. 4th at 733. In that situation, the entire letter was itself privileged. Under that analysis, witness statements contained within an attorney opinion letter would be protected as privileged. "The attorney-client privilege attaches to a confidential communication between the lawyer and the client and bars discovery of the communication irrespective of whether it contains unprivileged material." 47 Cal. 4th at 734. It was therefore improper to order production of the redacted letter.[2]

However, that analysis does not resolve the question of whether witness statements obtained in the course of an attorney investigation are protected against disclosure on work product or privilege grounds. Communications by corporate employees to attorneys representing the corporate entity are not always privileged: to make this determination, courts use a dominant purpose test. If the "corporation's dominant purpose in requiring the employee to make a statement is the confidential transmittal to the corporation's attorney of information emanating from the corporation, the communication is privileged." *D.I. Chadbourne, Inc. v. Superior Court*, 60 Cal. 2d 723, 737 (1964). "If the communication is privileged, it does not become unprivileged simply because it contains material that could be discovered by some other means."

[2] *Costco* also made clear that it was improper for the trial court to conduct an *in camera* review of the opinion letter in order to determine whether it was privileged. Evidence Code section 915 expressly prohibits such review. 47 Cal. 4th at 736.

Costco, 47 Cal. 4th at 735. This analysis would support the extension of privilege to statements provided by employee witnesses to attorneys during confidential investigations, where the dominant purpose of the communication is to secure legal advice.[3]

Even where that test is not met, however, the Court's work product analysis in *Coito* should apply. Witness statements obtained by an attorney, even of employee witnesses, constitute work product under *Coito*. To the extent the witness statements are "inextricably intertwined" with the attorney's thoughts and opinions, those will be more likely to be recognized by the court to constitute absolute work product, and not discoverable.

Conclusion

California case law has clarified the scope of the attorney-client privilege and work product doctrine. *Coito* enhances the work product protection applicable to witness statements obtained by attorneys, and applies regardless of the context in which such interviews take place.

About the Author: Merri A. Baldwin is a shareholder in the San Francisco office of Rogers Joseph O'Donnell P.C., where she focuses on business litigation and attorney liability and conduct, including legal malpractice, attorney-client fee disputes, ethics, professional responsibility and State Bar discipline defense. From 2011 to 2017 she served as a member of the State Bar of California Committee on Professional Responsibility and Conduct, She currently is a member of the Executive Committee of the Legal Malpractice section of the Bar Association of San Francisco, and is a lecturer at the University of California, Berkeley School of Law. She is the co-editor of a book published by the ABA, The Law of Lawyers' Liability. She can be reached at mbaldwin@rjo.com.

[3] At the same time, though, information does not become privileged simply because it is transmitted to an attorney. "[A] litigant may not silence a witness by having him reveal his information to the litigant's attorney . . ." *D.I. Chadbourne, Inc.*, 60 Cal. 2d at 734. Accordingly, the adverse party may interview the witness, or use interrogatories or deposition questioning in an effort to obtain the information that the witness provided to the attorney. *See Coito*, 54 Cal. 4th at 496.

NOTES

24

Steven E. Fagell, Benjamin S. Haley and Anthony Vitarelli, Covington & Burling LLP, Practical Guide for Maintaining Privilege Over an Internal Investigation (April 14, 2014)

Submitted by:
Merri A. Baldwin

Rogers Joseph O'Donnell

Kathryn J. Fritz

Fenwick & West LLP

Reprinted from the PLI Course Handbook,
Nineteenth Annual Institute on Privacy and Data Security Law (Item #219182)

I. INTRODUCTION

Imagine the following scenario:

Company X, with you as outside counsel, successfully navigates through a two-year DOJ and SEC investigation into potential Foreign Corrupt Practices Act ("FCPA") violations in multiple countries, culminating in favorable resolutions with both agencies. The investigation involved voluminous document productions, more than fifty interviews of current and former employees, deep-dive forensic accounting work by a "Big Four" firm, multiple presentations to the DOJ and SEC, and a host of remedial measures to address the issues under investigation, including the termination of a number of Company X's distributors, as well as employee terminations and discipline.

Barely after the ink dries on the settlement papers, Company X's Board of Directors receives a shareholder demand letter alleging that the Board breached its fiduciary duties by failing to adequately oversee the company's operations. Days later, the Board receives a letter from another shareholder demanding to inspect Company X's books and records, and specifically requesting, among other things, "all documents relating to the FCPA investigation, including, but not limited to, interview memoranda, presentations to the Government, and reports or memoranda reflecting the findings of the investigation."

As you review the shareholders' demands, you begin to assess whether Company X can claim privilege or work-product protection over the myriad documents that the shareholders' counsel have requested. A litany of questions runs through your head: Did you waive privilege by making witness proffers or other factual presentations to the DOJ and SEC? What about when you briefed the company's outside auditors? Are your communications to the company about termination of distributors and employee discipline protected? Were any privileged materials inadvertently produced, and did you take adequate steps to ensure the return of any such materials?

The answers to these questions will likely turn on decisions that were made years ago, and whether the company was attentive to the privilege traps inherent in internal investigations. Below, we discuss a number of these traps, and offer practical guidance on how to avoid them throughout the stages of an internal investigation. As we explain, decisions made at critical junctures of an investigation will determine whether Company X has adequately preserved applicable privileges and other protections.

II. THE BEGINNING OF AN INVESTIGATION

Preserving the privilege begins at the very outset of an investigation. Careful thought must be given to decisions regarding whom outside counsel represents, who will oversee the investigation, and whether and how to involve non-lawyers.

A. Be Clear on Who the Client Is and Who Is Overseeing the Investigation

To maintain privilege over an investigation, it is essential that outside counsel establish with clarity whom they represent and to whom they are reporting. In many cases, the issue will be relatively straightforward because outside counsel will be representing a company, and the investigation will be overseen by in-house counsel. Board committee investigations add a layer of complexity. While communications between a board committee and its counsel are the classic type of attorney-client communications that would generally be privileged, the case for protection of communications between committee counsel and other stakeholders in an investigation, such as company counsel (in-house or outside) and management, is less clear.[1]

Complications can also arise when an investigation (whether the client is the company itself or a board committee) involves allegations of wrongdoing by officers or directors, or when in-house counsel may have been involved in the conduct under investigation. An investigation may not be credible if it is overseen by the individuals whose conduct is at issue in the investigation. Leaving credibility issues aside, there are also very real waiver risks in such situations. For example, as discussed further below, if counsel reports the findings of an investigation to members of management or board members who have engaged in conduct that could make them adverse to the company, a waiver may result.[2] Additionally, particularly with respect to witness interviews, a lack of clarity over whether outside

1. *See, e.g.*, *Ryan v. Gifford*, Civil Action No. 2213-CC, 2007 WL 4259557, at *3 n.2 (Del. Ch. Nov. 30, 2007) (assuming, but not deciding, that a company could properly assert privilege over communications between the company and counsel to a special committee of the company's board).
2. *See, e.g.*, *id.* at *2-3. This issue can arise not only when counsel is reporting findings at the conclusion of an investigation, but also in circumstances where counsel is faced with requests from management to provide a briefing on the status of the investigation.

counsel represents both the company and individual directors and officers can have serious ethical and privilege implications.

To mitigate these risks, it may be desirable for outside counsel to be clear in their engagement letter about not only whom they represent, but also whom they *do not* represent. Additionally, outside counsel should be mindful that potential conflicts that are not apparent at the outset of an engagement may arise as facts are developed. For example, if, as an investigation progresses, it becomes apparent that the in-house counsel who is overseeing the investigation had substantive involvement in the events under investigation, outside counsel might consider recommending an alternative reporting line, or, if necessary, that oversight of the investigation be transferred to a board committee. These decisions are often complicated and highly sensitive, but outside counsel must satisfy itself from the outset that the engagement has been structured in a manner that most effectively safeguards the company's interests, including with respect to privilege.

B. Be Careful About Using Non-Lawyers to Conduct or Assist in an Investigation

Privilege traps can also arise when non-lawyers conduct or assist in an investigation. While non-lawyers, such as forensic accountants, often play a critical role in the fact-development process, careful thought must be given to how they are employed and how their work is overseen.

The use of a non-lawyer to lead an investigation carries with it the risk that the investigation will not be privileged. Recall that, for an investigation to be privileged, it must be shown that the investigation was conducted for the ultimate purpose of providing legal advice to the client. Because non-lawyers cannot provide legal advice, this predicate for the privilege may be lacking in an investigation led by a non-lawyer, even if counsel plays a role in advising on how to conduct the investigation.[3] Courts may well reject such an approach as a "gimmick" wherein counsel is not allowed to conduct the internal investigation but is retained "in a watered-down capacity to 'consult' on the investigation in order to cloak the investigation

3. *See, e.g., United States v. ISS Marine Servs., Inc.*, 905 F. Supp. 2d 121 (D.D.C. 2012) (holding that an investigation conducted by internal audit personnel was not covered by the attorney-client privilege and not protected by the work-product doctrine).

with privilege."[4] As one court has put it, "when an attorney is absent from the information-gathering process, 'the original communicator has no intention that the information be provided [to] a lawyer for the purposes of legal representation.'"[5]

If non-lawyers are employed to assist in an investigation, in order to maintain the privilege, it is critical that they act as agents for in-house or outside counsel, under the direction and control of such counsel, and for the purpose of assisting counsel in providing legal advice. The classic example of this is an accountant reviewing and analyzing a company's books and records to assist in an investigation.[6] There are several practical steps that counsel can take to help preserve the privilege in such circumstances.

First, if third-party consultants will be retained, it is preferable that outside counsel retain them directly, and that the purpose and nature of the engagement be memorialized in a written agreement. For example:

> This Statement of Work ("SOW"), effective as of [DATE], is made by [CONSULTANT] and [LAW FIRM] acting as agent for [CLIENT]. [CONSULTANT] understands and acknowledges that the services provided under this SOW are being requested by [LAW FIRM] on behalf of [CLIENT], and will be performed at the direction of [LAW FIRM] in order to assist [LAW FIRM] in providing confidential and privileged legal advice to [CLIENT].
>
> The parties understand that it is [LAW FIRM] and [CLIENT'S] intention that the work performed by [CONSULTANT] under this SOW will be covered by the attorney-client privilege, the attorney work-product doctrine, and all other applicable privileges and protections.

A separate SOW or engagement letter along these lines should be prepared for all third-party vendors, even if they regularly work for the client, including under a master services agreement.

Second, counsel should closely oversee and direct the work of consultants. To be sure, cost and efficiency considerations may dictate that communications between third-party consultants and company employees occur without counsel present. In this regard, it is not necessary for an attorney to "observ[e] and approv[e] every

4. *Id.* at 129.
5. *Id.* at 130 (quoting *Nesse v. Shaw Pittman*, 206 F.R.D. 325, 330 (D.D.C. 2002)).
6. *See, e.g., United States v. Kovel*, 296 F.2d 918, 922 (2nd Cir. 1961) (privilege applies to communications to an accountant retained by an attorney to assist in providing legal advice to the client).

minute aspect of [the consultant's] work."[7] That said, in order to maintain privilege, such communications should nonetheless be made "at the direction of counsel, to gather information to aid counsel in providing legal services."[8]

Third, consistent with these principles, if company employees are assisting in an investigation, they should be formally "deputized" by counsel, so that it is clear that they are working at counsel's direction in order to assist counsel in providing legal advice. The following is an example of a "deputizing" communication:

> Dear []:
>
> In response to a recent compliance hotline report, the Company has asked the Law Department to provide advice regarding the application of U.S. law to certain business conduct in the Company's operations in [COUNTRY X]. To provide this advice, the Law Department, with the assistance of outside counsel, will undertake a privileged and confidential investigation. I am writing to request your assistance in this matter in the preservation and collection of materials that may be relevant to this investigation, for the purpose of providing legal advice to the Company in this matter. In assisting in this investigation, you will be acting under the direction of the Law Department and its outside counsel in providing legal services to the Company.
>
> Any and all communications relating to this investigation are privileged and confidential, and neither those communications nor the fact of this investigation should be disclosed to anyone other than Company or outside counsel or others to whom Company counsel has authorized disclosure. Additionally, any materials or information collected in the course of this investigation should be treated as confidential, and should not be disclosed to anyone except at the express direction of Company or outside counsel.

C. Make Clear that the Purpose of the Investigation Is to Provide Legal Advice

If a company or a board committee intends to maintain privilege over an internal investigation, it should say so explicitly. This can be accomplished through various means—*i.e.*, in board minutes, through an email, orally if later memorialized in a file memo, or through a more formal, direct communication from management or the board authorizing counsel to undertake an investigation for the purpose of providing legal advice. If possible, in order to help substantiate a

---

7. *See Gucci Am., Inc. v. Guess?, Inc.*, 271 F.R.D. 58, 72 (S.D.N.Y. 2010) (quoting *In re Rivastigmine Patent Litig.*, 237 F.R.D. 69, 81 (S.D.N.Y. 2006)).
8. *Id.* at 80.

claim for protection under the work-product doctrine, the communication should identify actual or anticipated litigation or Government investigations arising from the conduct under investigation. The following is an example of a formal communication achieving this objective:

> To: General Counsel
>
> From: Chief Executive Officer
>
> Re: Investigation of Matters in [COUNTRY X]
>
> In response to a recent compliance hotline report and press reports, I am requesting the Law Department to provide advice regarding the application of U.S. law to certain business conduct in the Company's operations in [COUNTRY X]. To provide this advice, I am requesting that the Law Department, with the assistance of outside counsel, undertake a privileged and confidential investigation.
>
> The events at issue have already given rise to a number of shareholder demand letters threatening litigation, and a request to inspect the Company's books and records. We are also aware of several law firms that have issued press releases indicating that they are investigating potential claims against the Company under U.S. securities laws. Additionally, we expect that the events that are the subject of the hotline and press reports will attract the attention of U.S. and foreign law enforcement authorities, including the Securities and Exchange Commission and the Department of Justice. The Company is seeking legal advice in connection with these matters, in anticipation of litigation, and the investigation is necessary so that you can provide this advice.
>
> Any and all communications relating to this investigation and the requested legal advice are privileged and confidential, and neither those communications nor the fact of this investigation should be disclosed to anyone other than Company or outside counsel or others to whom Company counsel has authorized disclosure. Additionally, any materials or information collected in the course of this investigation should be treated as confidential, and should not be disclosed to anyone except at the express direction of Company or outside counsel.

This type of formal communication has the advantage of establishing and articulating the purpose of the investigation in a manner that is best protective of the privilege. Ideally, the purpose of the investigation should be clearly articulated early and often as the investigation proceeds—for example, when counsel seeks assistance from company personnel in preserving and collecting data, in *Upjohn*[9] warnings during witness interviews, in presenting findings to management or the board, and, if necessary, when interacting with

9. *See Upjohn Co. v. United States*, 449 U.S. 383 (1981).

enforcement authorities. In other words, it should be clear from the entire record of the investigation that outside counsel had been retained to conduct an investigation for the purpose of providing the company with legal advice. The existence of such a record will help a company to rebut an argument that no privilege attached to the investigation.[10]

D. Be Sensitive to the Complexities of Privilege Issues Outside the United States

If the subject matter of an internal investigation has the potential to draw the attention of foreign regulators or litigants, counsel cannot safely assume that United States law will govern subsequent adjudications of privilege issues. In a number of foreign jurisdictions, in-house counsel do not enjoy the same privilege and work-product protections as in the United States. For instance, in 2010, the European Court of Justice held in *Akzo Nobel Chemicals Ltd. v. European Commission* that, because in-house counsel are unable to exercise independence from the companies that employ them, their communications with the company are not privileged.[11] Thus, for investigations that may ultimately be the focus of litigation in the European Union, companies should evaluate the privilege risks that flow from having in-house lawyers lead such investigations. As a more general matter, in light of the differing legal standards that operate in foreign jurisdictions, counsel should take time at the outset of an investigation to research the relevant jurisdiction's privilege law when deciding which personnel will conduct which aspects of the investigation.

III. THE MIDDLE OF AN INVESTIGATION

The fact-development stage of an investigation—conducting interviews, reviewing and producing documents, coordinating with other attorneys, and providing advice to the client—presents numerous risks to the privilege. We consider here some of the risks related to interviews,

---

10. *See, e.g.*, *United States ex rel. Barko v. Halliburton Co.*, No. 1:05-CV-1276, Slip Op. at 5 (D.D.C. Mar. 6, 2014) (declining to find investigations privileged where they were "undertaken pursuant to regulatory law and corporate policy rather than for the purpose of obtaining legal advice").
11. Case C-550/07P, *Akzo Nobel Chems. Ltd. & Ackros Chems. Ltd. v. Comm'n*, 2010 E.C.R. I-08301.

productions of documents, joint defense or common interest agreements, and the provision of advice on issues ancillary to an investigation.

A. Carefully Consider the *Upjohn* Warning

Conducting effective interviews is an essential element of a thorough investigation. Preserving the company's privilege, however, requires that attorneys give an adequate *Upjohn* warning before beginning the interview. If an attorney glosses over the warning or leaves out key aspects of it, he or she may jeopardize the privileged nature of the interview. In contrast, if an attorney takes an overly prosecutorial tone in delivering the warning, the attorney may chill the witness's willingness to cooperate fully, or even at all.

As a technical matter, the *Upjohn* warning should cover the following points:

- I am a lawyer for the company and do not represent you personally.
- The purpose of the interview is to learn about [the issue] in order to provide legal advice to the company.
- This conversation is privileged, but the privilege belongs to the company, not you. It is up to the company whether to waive the privilege, including with respect to the Government or other third parties.
- The conversation should be kept confidential in order to preserve the company's privilege.

Once those foundational points have been made clear, attorneys should inquire whether the witness has any questions. Before moving to the substantive focus of the interview, attorneys should receive a clear affirmation that the witness understands the warning and is willing to proceed with the interview.

If delivered effectively, the *Upjohn* warning will adequately advise the witness of the implications of the interview, without chilling the witness's willingness to cooperate. The following are some practical tips that can lead to cooperative, privileged interviews:

- Confer with the client in advance of interviews to understand whether particular witnesses present any unique sensitivities. In such circumstances, it may be helpful for in-house counsel or the employee's manager to have a brief discussion with the employee

outside the presence of outside counsel in order to provide some context for the interview.

- Do not deliver the *Upjohn* warning in a rote, mechanized way; be friendly and casual. The witness should not feel like he or she is being read a *Miranda* warning.
- Emphasize the importance of the investigation to the company and the need for complete and accurate information. Express appreciation for the witness's assistance in helping the company to understand the relevant facts.
- If applicable, explain that the company is interviewing a number of individuals and is not singling out that particular employee.

Once counsel has delivered the *Upjohn* warning and obtained the witness's agreement to proceed, the content of the interview will be protected by the attorney-client privilege, so long as the attorney and the witness keep its content confidential. As an additional precaution, counsel should remind the witness at the conclusion of the interview not to discuss the substance of the interview with anyone else, except to the extent that the witness wishes to convey additional information or to ask follow-up questions. Such follow-up communications should be directed to an appropriate contact in the company's legal department or, depending on the circumstances, to outside counsel directly.

The risks of failing to give an adequate *Upjohn* warning can be severe. The 2009 case *United States v. Ruehle*[12] provides a stark example. *Ruehle* involved a DOJ and SEC investigation into alleged stock-option backdating at Broadcom Corporation. In the course of Broadcom's internal investigation, its outside counsel interviewed William Ruehle, Broadcom's CFO. During the interview, Ruehle made numerous statements that he later sought to suppress as privileged in his criminal trial. Ruehle argued that because outside counsel had represented Ruehle and other individual officers in shareholder suits and had failed to advise him during the interview that his statements could be disclosed to third parties, his statements in the interview were privileged. The district court agreed. The court suppressed Ruehle's statements from the interview, concluded that outside counsel had breached their duty of loyalty to Ruehle, and

12. 583 F.3d 600 (9th Cir. 2009).

referred the lawyers involved to the California State Bar for possible discipline.[13]

In reaching its decision, the district court concluded that there was no record that an adequate *Upjohn* warning had been provided, relying, among other things, on the fact that there was no reference to an *Upjohn* warning in the interviewing attorneys' notes.[14] The court went on to note that even if it credited one of the interviewing attorneys' testimony that he had given an *Upjohn* warning, the warning was inadequate because the attorneys failed to advise Ruehle that they were not acting as his counsel during the interview, or that "any statements he made to them could be shared with third parties, including the Government in a criminal investigation."[15] While the Ninth Circuit ultimately overturned the district court's privilege ruling on the ground that Ruehle knew his statements would be disclosed to the company's auditors—and thus were not confidential—this case illustrates the problems that can occur when there is a lack of clarity about whom outside counsel represents and when attorneys fail to provide adequate *Upjohn* warnings.[16]

B. Carefully Consider the Scope of Interviews Involving Former Employees

Counsel must be particularly sensitive to privilege considerations when conducting interviews of former employees. Federal courts generally have held that communications with former employees about events that occurred within the scope of their prior employment are subject to the attorney-client privilege.[17] Counsel conducting an

13. *United States v. Nicholas*, 606 F. Supp. 2d 1109 (C.D. Cal. 2009), *rev'd sub nom. United States v. Ruehle*, 583 F.3d 600.
14. *Nicholas*, 606 F. Supp. 2d at 1116.
15. *Id.* at 1117.
16. *See Ruehle*, 583 F.3d at 602.
17. *See Upjohn Co. v. United States*, 449 U.S. 383, 403 (1981) (Burger, C.J., concurring) ("[A] communication is privileged at least when . . . an employee or former employee speaks at the direction of the management with an attorney regarding conduct or proposed conduct within the scope of employment"); *In re Allen*, 106 F.3d 582, 605 (4th Cir. 1997) ("Most lower courts have followed the Chief Justice's reasoning and granted the privilege to communications between a client's counsel and the client's former employees."). *But see id.* at 606 n.14 (citing federal cases denying the privilege as to communications with former employees and describing them generally as either "following state law" or having concluded that "the former employee had ceased being employed by the client *before* the relevant conduct occurred").

investigation should thus use great care to focus the interview on matters that occurred during the former employee's tenure, as some district courts have held that interviews on topics subsequent to employment with the company are not privileged.[18]

Counsel also should consider the circumstances of the witness's departure from the company when assessing whether the witness is likely to be cooperative or to maintain the confidentiality of the interview. In the absence of a contractual provision (*e.g.*, in a severance agreement) obligating an employee to cooperate in an investigation and maintain confidentiality, a company may have no effective remedy against a former employee who fails to maintain confidentiality. Even with such contractual protections, their utility may be limited; the SEC, for example, has made clear that such contractual undertakings cannot be used to prevent someone from reporting information to the Commission under the Dodd-Frank Wall Street Reform and Consumer Protection Act.[19] Thus, if a company has real concerns that the employee will not maintain confidentiality, it should think carefully about whether to proceed with the interview.

C. Draft Interview Summaries or Memoranda with an Eye to Preserving Privilege

Memorializing the content of the interview is essential to a credible investigation. When crafted well, interview summaries should avoid the need to revisit topics with witnesses and can serve as a resource to the rest of the investigative team. To ensure that the content of such summaries remains privileged, interviews should not be recorded or transcribed verbatim. A recorded or transcribed interview summary will be considered more easily discoverable than a written summary that contains an attorney's mental impressions.[20] The summary should state expressly that it does not constitute a transcript and that the content is not presented sequentially. Moreover, the written summary should state that it contains the thoughts, mental impressions, and conclusions of the attorney. The written summary also should confirm that the *Upjohn* warning was delivered, describe the content of the warning, and indicate that the witness understood

18. *See, e.g.*, *United States ex rel. Hunt v. Merck-Medco Managed Care, LLC*, 340 F. Supp. 2d 554, 558 (E.D. Pa. 2004); *Peralta v. Cendant Corp.*, 190 F.R.D. 38, 41 (D. Conn. 1999).
19. *See* 17 C.F.R. § 240.21F-17(a) (2012).
20. *See* FED. R. CRIM. P. 26.2(a), (f)(2).

and agreed to proceed with the interview. Sample introductory language to a typical written interview summary follows:

> On [DATE], [names of counsel] met with and interviewed [WITNESS], [TITLE] of Company X (the "Company"), at [LOCATION]. This memorandum consists of information obtained in the course of the interview as well as the thoughts, impressions and conclusions of counsel. The memorandum is not and is not intended to be a verbatim transcript of the interview and in many instances is organized topically, rather than in the sequence in which the conversation took place. This memorandum has not been reviewed by [WITNESS] for accuracy or otherwise adopted by him as his statement.
>
> At the outset, counsel explained that Company X is concerned about the possibility that certain laws may have been violated in connection with specific areas of Company X's business and that [LAW FIRM] had been hired to look into the situation and to give the Company legal advice. Counsel told [WITNESS] that [LAW FIRM] is representing the Company in this matter, not him personally, but that his help is needed to collect and understand the facts so that the Company can receive accurate advice. Counsel also explained that the conversation was privileged, but it was up to the Company to decide whether it would like to disclose what was discussed to a third party or to the Government. Counsel told [WITNESS] not to talk to anyone else about this meeting or about what was discussed. He confirmed that he understood all of the above.

D. Use Clawback Provisions to Prevent Waiver from Inadvertent Production of Privileged Materials

Few experienced practitioners have avoided entirely the problem of an inadvertently disclosed privileged document. The scope, scale, and complexity of investigations today create a significant risk of inadvertent production of privileged material. To mitigate that risk, document production letters should include unequivocal language, preserving the client's ability to recover inadvertently disclosed documents. Sample language follows:

> It is possible that, despite our diligent efforts, certain information protected by [our client's] attorney-client privilege or other applicable privileges may have been included in this production. Accordingly, we hereby reserve our right to seek the return of any privileged or protected materials that may have been inadvertently produced, and respectfully advise you that any inadvertent production should not be considered a waiver. We respectfully request that you inform us immediately if you become aware of any such materials in our production.

Of course, no language is a substitute for a painstaking privilege review of all documents in advance of production, but incorporating this language can ensure that any documents escaping such a review can be recovered without effectuating a privilege waiver.

E. Joint Defense Agreements Should Have Language that Protects Privileged Communications

Sharing of information among counsel for clients with a common interest can yield substantial efficiencies and may be helpful in developing an accurate and comprehensive understanding of the facts. Doing so, however, can imperil the privilege, as such collaboration will often involve the disclosure of confidential information. Joint defense or common interest agreements address this concern by bringing confidential communications among outside counsel and their clients within the ambit of the attorney-client privilege and the work-product doctrine. Carefully drafting joint defense agreements will ensure that attorneys can conduct an efficient investigation with other outside counsel, while preserving the privilege and other applicable protections. Some tips on drafting these agreements follow:

- Meticulously define the scope of the common interest and thus the scope of the agreement.
- Indicate that the parties may, at their discretion, share information concerning the relevant matters without waiving any applicable privileges.
- Note that nothing in the agreement—nor the simple sharing of information pursuant to the agreement—shall constitute a waiver of any applicable privilege or protection.
- Include clawback language regarding inadvertent disclosures of privileged information.
- Provide for unilateral withdrawal from the agreement by any party for any reason, while noting that the agreement will continue to protect all shared information prior to withdrawal.

F. Be Wary of Providing Non-Legal Advice

In any internal investigation, outside counsel may be asked to advise on topics that are ancillary to the core legal issues under investigation. A prominent example is advice on issues relating to termination of commercial relationships or employee discipline. In light of recent case law, counsel should be aware that the provision of "business advice"—even in the context of a privileged investigation—may not itself be privileged. For example, in the 2014 case *Koumoulis v. Independent Financial Marketing Group, Inc.*, the plaintiffs sought to compel production of communications between

the defendants and their outside counsel regarding the internal investigation of plaintiff's discrimination claims.[21] The defendants withheld the documents, asserting the attorney-client privilege and work-product protection. Although these documents seem like core privileged communications, the district court did not find clearly erroneous a magistrate's finding that "their predominant purpose was to provide human resources" advice; the district court accordingly held that no attorney-client privilege attached.[22] The district court explained that "almost all of the information contained in the [documents] relates to business advice provided by outside counsel to Defendants' human resources personnel or the factual record of Defendants' internal investigation."[23] For similar reasons, the court explained that work-product protection did not apply: While "it may be true that the possibility of litigation prompted Defendants to seek outside counsel's advice, the communications themselves demonstrate that rather than discussing litigation strategy or advice, [outside counsel] advised Defendants on how to conduct the internal investigation," as well as on how to address plaintiff's "ongoing work performance issues and internal complaints," which is "advice that would have been given regardless of a specific threat of litigation."[24]

This decision makes clear that there is a real disclosure risk in providing advice of a "business-related character" when assisting clients in conducting an internal investigation.[25] Any such communications not only should be labeled with privilege legends, but also should include more than "a stray sentence or comment within an e-mail chain referenc[ing] litigation strategy or advice."[26] Communications related to the structure and scope of an internal investigation must be continually tied back to the provision of legal advice and the prospect of future litigation.

21. *Koumoulis v. Indep. Fin. Mktg. Grp.*, No. 10-CV-0887, 2014 WL 223173 (E.D.N.Y. Jan. 21, 2014).
22. *Id.* at *3-5.
23. *Id.* at *2.
24. *Id.* at *6.
25. *Id.* at *4.
26. *Id.*

IV. THE END OF AN INVESTIGATION

The conclusion of an internal investigation—particularly one that will inform the Government's decision on whether to bring an enforcement action—will often involve some form of reporting that may implicate a variety of privilege considerations. We consider here the risks related to such reporting, the issue of "selective waiver," and the issues to consider in communicating with a company's outside auditors about an internal investigation.

A. When Reporting Findings, Carefully Consider the Audience and Method of Reporting

The manner in which outside counsel elects to report the findings of the internal investigation has significant consequences for the privilege. For some investigations, attorneys will have little choice regarding the form of disclosure, as the investigation will inexorably lead to some public disclosure of findings (*e.g.*, a major scandal of broad national or international interest). In contrast, other investigations are conducted with the expectation that the findings will remain closely held by the client. Between those two poles are internal investigations conducted in parallel with Government investigations, in which attorneys are expected to proffer factual information learned during the course of their investigation.

Reporting in the context of a Government investigation presents a unique form of risk, given the possibility of a broad subject-matter waiver of the privilege. To guard against this risk, counsel is typically well served both to limit the disclosure of investigative findings (whether delivered orally or in writing) to those audiences with a need to know, and to be clear that such communications are confidential (through, for example, appropriate use of legends calling for protection from disclosure under the Freedom of Information Act). Additionally, counsel should be mindful that subject-matter waiver occurs only when there is a voluntary disclosure of *privileged* information. This counsels in favor of limiting investigative reports or presentations—to the extent possible—to a detailed recitation of the investigative process and the relevant facts. If counsel is able to avoid preparing a written report and can instead prepare a presentation consisting of source documents, coupled with an oral presentation of relevant facts, the risk of a privilege waiver can be substantially mitigated.

As noted above, special attention must be given to the risk of waiver in circumstances where counsel is communicating findings to potentially adverse parties. For example, if outside counsel has been retained by a board committee and subsequently presents to the entire board, there is a risk of waiver to the extent the facts suggest the board members did not receive and consider the presentation in their roles as fiduciaries of the company, but rather in their personal capacities as defendants (potential or actual) in litigation.[27]

A 2007 Delaware case, *Ryan v. Gifford*, illustrates the point. In *Ryan*, the Delaware Chancery Court found a subject-matter waiver where a special committee's findings were disclosed to the full board, including board members who were defendants in the underlying derivative suit and whose personal counsel attended the presentation.[28] The court concluded that since the committee's disclosure was made to the defendant board members in their individual capacities as defendants (and subjects of the special committee investigation) rather than in their fiduciary capacities as board members, the common interest doctrine did not apply.[29] While it should not be read for the proposition that counsel to a special committee always effectuates a privilege waiver by communicating its investigative findings to the full board, *Ryan* reinforces the notion that counsel must tread cautiously in this area.[30]

---

27. *See, e.g., In re OM Sec. Litig.*, 226 F.R.D. 579, 593 (N.D. Ohio 2005) (finding a privilege waiver when counsel for the Audit Committee presented a report to the full board).
28. *Ryan v. Gifford*, Civil Action No. 2213-CC, 2007 WL 4259557, at *3 (Del. Ch. Nov. 30, 2007) ("The presentation of the report constitutes a waiver of privilege because the client, the Special Committee, disclosed its communications concerning the investigation and final report to third parties—the individual director defendants and Quinn Emmanuel—whose interests are not common with the client, precluding application of the common interest exception to protect the disclosed communications.").
29. *Id.*
30. In a subsequent opinion denying a motion for an order certifying an interlocutory appeal, the court explained the potentially limited reach of its opinion: "The decision would not apply to a situation (unlike that presented in this case) in which board members are found to be acting in their fiduciary capacity, where their personal lawyers are not present, and where the board members do not use the privileged information to exculpate themselves." *Ryan. v. Gifford*, Civil Action No. 2213-CC, 2008 WL 43699, at *5 (Del. Ch. Jan. 2, 2008).

B. Even Oral Proffers Risk a Waiver

Oral proffers are frequently employed to provide Government enforcement authorities with factual information gathered in an internal investigation. Although this tactic can alleviate the risk of handing over a written document memorializing the results of a privileged investigation, there is still danger in making oral proffers.

This risk was made clear in *SEC v. Vitesse Semiconductor Corp.*, in which outside counsel for a non-party company's audit committee had delivered to the SEC oral summaries of multiple witness interviews, which concerned the conduct of the defendants in the SEC enforcement action.[31] When the defendants learned of notes from these witness interviews and moved to compel their production, the non-party company asserted privilege. To assess whether the proffer constituted a waiver of work-product protection, the district court conducted an *in camera* review of counsel's handwritten notes of the witness interviews and the notes of an SEC lawyer who had taken notes during the oral proffer.[32] The court found that "the oral summaries provided to the SEC were very detailed" and were "witness-specific"; at times, "the SEC's notes matched [company counsel's] notes almost verbatim."[33] Accordingly, the district court concluded that the company had waived work-product protection and ordered the company to turn over the notes because it had "effectively produced these notes to the SEC through its oral summaries."[34]

Companies, therefore, should exercise caution as they approach factual proffers based on witness interviews. In that regard, counsel should have a written understanding in place with the relevant governmental agency that the factual proffer is not intended to effect a waiver. Moreover, counsel should consider other means to avoid an inadvertent waiver, such as not providing verbatim recitations of witness interviews and attempting instead to proffer facts surrounding particular issues under investigation, drawing on the witness interviews and other sources to inform the proffer.

---

31. No. 10 Civ. 9239, 2011 WL 2899082, at *1-3 (S.D.N.Y. July 14, 2011).
32. *Id.* at *3.
33. *Id.*
34. *Id.*; *see also Gruss v. Zwirn*, 09 Civ. 6441, 2013 WL 3481350 (S.D.N.Y. July 10, 2013) (finding a work-product waiver where counsel "deliberately, voluntarily, and selectively disclosed to the SEC" summaries of twenty-one witness interviews in a PowerPoint presentation).

C. Do Not Rely on "Selective Waiver"

Reporting only on the facts learned in an investigation may not provide a sufficiently comprehensive account to the Government to preclude an indictment or to achieve an otherwise favorable resolution. In these circumstances, a company may conclude that the benefits of full disclosure outweigh the costs of waiving the privilege. If the client makes this determination, outside counsel may still hope to effect only a "selective waiver," whereby privileged information is disclosed to the Government yet remains protected from disclosure to third parties. Selective waiver, however, is disfavored in most federal courts of appeals and has been adopted only by the Eighth Circuit.[35]

If the company does intend to disclose privileged material to the Government, it should first attempt to obtain an agreement from the Government that it will keep the information confidential (a "McKesson letter"). Future plaintiffs, however, will not be parties to this agreement, and some courts have found that productions of privileged materials pursuant to confidentiality agreements with the Government nonetheless constitute a waiver.[36] Notwithstanding the risk, these agreements can still be worthwhile because they limit the chance that the Government will argue that a voluntary production constitutes a waiver; moreover, privately held companies do not face the same risks as publicly traded companies with respect to downstream litigation. Simply put, a confidentiality agreement is beneficial, but even with an ironclad agreement in place, companies should not expect that materials produced to the Government will be immune from subsequent disclosure in civil litigation.

---

35. *Compare Diversified Indus., Inc. v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1978) (en banc) (adopting doctrine of selective waiver because "[t]o hold otherwise may have the effect of thwarting the developing procedure of corporations to employ independent outside counsel to investigate and advise them in order to protect stockholders, potential stockholders and customers"), *with In re Pac. Pictures Corp.*, 679 F.3d 1121, 1127-28 (9th Cir. 2012) (rejecting selective waiver and collecting cases for the proposition that the doctrine had been "rejected by every other circuit to consider the issue since" the Eighth Circuit considered it in *Diversified Industries*).
36. *See, e.g.*, *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 302-04 (6th Cir. 2002); *Westinghouse Elec. Corp. v. Republic of Phil.*, 951 F.2d 1414, 1424-27, 1431 (3d Cir. 1991). *But see Saito v. McKesson HBOC, Inc.*, No. Civ.A. 18553, 2002 WL 31657622, at *11 (Del. Ch. Nov. 13, 2002) ("I adopt a selective waiver rule for disclosures made to law enforcement agencies pursuant to a confidentiality agreement.").

D. Exercise Care in Communications with Outside Auditors

As a general matter, disclosure of privileged information to external auditors constitutes a subject-matter privilege waiver.[37] Auditors, however, typically recognize that demanding privileged information would put the company in an untenable position, and they are often receptive to a company's waiver concerns. To the extent that auditors have continued to request more detailed information in the wake of high-profile accounting fraud cases, companies need to be prepared to communicate with their auditors about internal investigations in a way that will not constitute a waiver of the privilege. Some tips follow:

- Consider briefing the auditors from the outset of the investigation. Have a candid conversation with them about the need for outside counsel to maintain privilege, while still providing them the information they require to perform their procedures. Enlist the help of the general counsel, the head of the internal audit department, or other appropriate in-house personnel to facilitate the dialogue between outside counsel and the independent auditors.
- Focus on process. Without revealing privileged legal advice, provide the auditor detailed information about the investigative process—the investigation's structure, the personnel involved, the document preservation steps that were taken, the number of interviews conducted, the number of documents reviewed, the outside accountants and vendors employed, and any other relevant information. The stronger the investigative process and the more complete the description of the process, the more likely it is that the auditors will feel comfortable with the reliability of the investigation.
- If necessary, provide factual proffers to the auditors orally, rather than in a written, discoverable document.

Finally, while the disclosure of privileged information to auditors will likely waive the attorney-client privilege, work-product protection may remain intact because the auditor is not adverse to the client. For instance, in *Merrill Lynch & Co. v. Allegheny Energy, Inc.*, Allegheny sought to compel discovery of two internal investigation reports (prepared by in-house and outside counsel), which Merrill

37. *See, e.g., Chevron Corp. v. Pennzoil Co.*, 974 F.2d 1156, 1162 (9th Cir. 1992).

Lynch had disclosed to its auditor.[38] Allegheny argued that the disclosure waived any applicable privilege.[39] The district court disagreed, stating that the "critical inquiry" is whether the auditors "should be conceived of as an adversary or a conduit to a potential adversary."[40] The court held that "any tension between an auditor and a corporation that arises from an auditor's need to scrutinize and investigate a corporation's records and book-keeping practices simply is not the equivalent of an adversarial relationship contemplated by the work product doctrine."[41] Although this view is not universally held,[42] if the client cannot avoid disclosure of privileged information to its auditors, counsel should zealously argue in subsequent civil litigation that work-product protection remains intact.

V. CONCLUSION

The consequences of a privilege or work-product waiver can be significant. It is therefore critical that attorneys conducting privileged internal investigations remain continually focused not only on conducting a credible, comprehensive investigation, but also on doing so in a manner that ensures the integrity of the attorney-client privilege, attorney work-product protection, and other applicable privileges and protections. This article has explained that pitfalls with respect to waiver exist at every stage of an internal investigation. Nonetheless, with careful planning and vigilance, attorneys can guide their clients safely through an internal investigation, while minimizing these downstream risks.

---

38. 229 F.R.D. 441 (S.D.N.Y. 2004).
39. *Id.* at 444.
40. *Id.* at 447.
41. *Id.* at 448.
42. *Compare SEC v. Schroeder*, No. C07-03798, 2009 WL 1125579, at *8-9 (N.D. Cal. Apr. 27, 2009) (following *Merrill Lynch* and finding work-product protection applied to documents that had been disclosed to a company's auditors), *and SEC v. Roberts*, 254 F.R.D. 371, 381-82 (N.D. Cal. 2008) (same), *with Medinol, Ltd. v. Boston Scientific Corp.*, 214 F.R.D. 113, 116 (S.D.N.Y. 2002) (holding that disclosure of the meeting minutes of a Special Litigation Committee to the company's auditors waives work-product protection because the disclosure "did not serve any litigation interest . . . or any other policy underlying the work product doctrine" and because the auditors' interests "were not necessarily united with those of" the company), *and United States v. Hatfield*, No. 06-CR-0550, 2010 WL 183522, at *3-4 & n.4 (E.D.N.Y. Jan. 8, 2010) (noting that "most courts have concluded that disclosure to an independent auditor does not waive the work product immunity" but nonetheless following *Medinol*).

NOTES

NOTES

25

The State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2012-183

Submitted by:
Merri A. Baldwin

Rogers Joseph O'Donnell

Kathryn J. Fritz

Fenwick & West LLP

THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2012-183

ISSUE: May an attorney disclose client confidences to her own attorney to evaluate a wrongful discharge action against her former firm and, in pursuing her claim, may she or her attorney publicly disclose those client confidences?

DIGEST: While an attorney may disclose client confidences to her own attorney to evaluate a potential wrongful discharge claim against her former firm, neither she nor her attorney may publicly disclose those confidences except in the narrowest of circumstances.

AUTHORITIES INTERPRETED: Rules 1-120, 3-100, and 3-110 of the Rules of Professional Conduct of the State Bar of California.[1/]

Business and Professions Code section 6068, subdivision (e)(1) and (e)(2).

STATEMENT OF FACTS

Senior Associate engages Attorney to represent her in a potential wrongful discharge action against her former Firm. If litigation ensues, embarrassing confidential information about at least one Firm client might need to become public because the information is inextricably bound to the core of Senior Associate's wrongful discharge claim. Attorney believes Senior Associate has a valid claim, but both are concerned that pursuit of such a claim could lead to violations of their professional responsibilities with respect to confidential information of the Firm's clients and may not be permissible.

DISCUSSION

1. Senior Associate's duty of confidentiality to Firm's client does not bar her right to seek legal advice.

Senior Associate has a duty of confidentiality to her former clients. (Bus. & Prof. Code, § 6068(e)(1) (duty to "maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client"); rule 3-100(A) ("A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) without the informed consent of the client, or as provided in paragraph (B) of this rule").)[2/]

The duty of confidentiality continues even after termination of the attorney-client relationship. The term "client," as used in both section 6068(e) and the attorney-client privilege (see Evid. Code, §§ 950, *et seq*.), applies to both present and former clients. (See, e.g., *Wutchumna Water Co. v. Bailey* (1932) 216 Cal. 564, 571 [15 P.2d 505] (attorney's lips are sealed forever, notwithstanding client's discharge of lawyer); *David Welch Co. v. Erskine & Tully* (1988) 203 Cal.App.3d 884, 890 [250 Cal.Rptr. 339]; *Commercial Standard Title Co. v. Sup. Ct. (Smith)*

[1/] Unless otherwise noted, all rule references are to the Rules of Professional Conduct of the State Bar of California.

[2/] According to the Discussion, comment [2] of rule 3-100: "The principle of client-lawyer confidentiality applies to information relating to the representation, whatever its source, and encompasses matters communicated in confidence by the client, and therefore protected by the attorney-client privilege, matters protected by the work product doctrine, and matters protected under ethical standards of confidentiality, all as established in law, rule and policy. (See *In The Matter of Johnson* (Rev. Dept. 2000) 4 Cal. State Bar Ct. Rptr. 179; *Goldstein v. Lees* (1975) 46 Cal.App.3d 614, 621 [120 Cal. Rptr. 253].)"

(1979) 92 Cal.App.3d 934, 945 [155 Cal.Rptr. 393] (duty owed to present and former clients); see also rule 3-310(E).) As a consequence, Senior Associate must guard against disclosure of client confidential information unless otherwise permitted by law.

Does this duty, however, prevent Senior Associate from seeking legal advice from Attorney and in doing so, disclosing to Attorney client confidential information?

Notwithstanding section 6068(e)(1) and rule 3-100(A), case law would permit Senior Associate to disclose confidential information both about the Firm and the Firm's client to Attorney to obtain legal advice about her rights against the Firm. (See *Fox Searchlight Pictures, Inc. v. Paladino* (2001) 89 Cal.App.4th 294, 308-315 [106 Cal.Rptr.2d 906].)

In *Fox Searchlight*, the court held that a former in-house counsel could disclose to her attorney all facts relevant to her termination, including employer confidences and privileged communications, in order to seek advice about, and to prosecute, a wrongful termination lawsuit against her former employer-client. *Id*. at p. 308. The court, however, added this caveat:

> In the present case we are not faced with, and do not decide, whether the former in-house counsel or her attorney can be held liable to the employer for the *public* disclosure of those confidences and communications. *Id.* (emphasis added).

The *Fox Searchlight* court reasoned that the California Supreme Court in *General Dynamics v. Superior Court* (1994) 7 Cal.4th 1164 [32 Cal.Rptr.2d 1] contemplated that, in a wrongful termination case, a limited disclosure of employer-client confidences to the plaintiff's own attorney is necessary. In addition, *Fox Searchlight* recognized that the attorneys for the in-house counsel were themselves bound by the rules of confidentiality and attorney-client privilege and, thus, disclosure to them would not be a *public* disclosure. *Fox Searchlight, supra,* 89 Cal.App.4th at p. 311.

The *Fox Searchlight* court also focused on the practical result of such consultation. Given the warnings in *General Dynamics* about public disclosure of client confidences, except in the most limited circumstances, in-house counsel must consider whether she can assert her claims without publicly disclosing the employer's confidences or, if not, whether she has an applicable exception to the confidentiality requirement. In such circumstances, *Fox Searchlight* held that in-house counsel "should be permitted to seek out independent, candid, professional advice about their ethical duties under their particular circumstances." *Id.* at p. 312. The court added:

> Indeed, the employer's confidentiality would seem better protected if, early on, in-house counsel consults her own attorney about the ethical issues in a wrongful termination case rather than risk having confidential communications disclosed inadvertently in the later stages of the litigation. *Id*., *citing, inter alia*, Model Rule 1.6(b)(2).

Thus, *Fox Searchlight* makes clear that lawyers have the right to disclose employer-client confidential information when seeking legal advice from their own lawyers whether for their own protection or in aid of the client's cause. *Fox Searchlight*, *supra*, 89 Cal.App.4th at pp. 313-314.

In *Fox Searchlight*, the client was the employer against whom in-house counsel wished to assert a wrongful discharge claim. That court deemed the employer-client confidential information necessary for her lawyer to evaluate her potential claims. *Id.* at p. 310. Here, however, Senior Associate's claim is against her former Firm, a claim she believes will necessarily implicate the confidential information of at least one Firm client. The client itself will not be a party to the wrongful discharge action. Under our facts, Firm client's confidential information is necessary for Attorney to evaluate Senior Associate's claim against Firm, and to properly to advise her. We conclude that *Fox Searchlight* and *General Dynamics* permit Senior Associate to reveal only so much of the Firm client's confidential information to Attorney as is necessary for him to evaluate her potential claims against Firm.

Solin v. O'Melveny & Myers, LLP (2001) 89 Cal.App.4th 451 [107 Cal.Rptr.2d 456]—decided two days after *Fox Searchlight* by a different division of the same Court of Appeal—impliedly reinforces a limited right to privately reveal a client's confidential information. In *Solin,* Solin (an attorney) consulted with his own counsel at O'Melveny about, *inter alia*, potential criminal liability in his continued representation of his clients. Although the heart of the dispute was O'Melveny's need to disclose that third-party client's confidential information in its defense

of Solin's subsequent malpractice action against the firm, neither the trial court nor the Court of Appeal expressed any concern that Solin had revealed his clients' confidences to his counsel at O'Melveny.

Thus, we conclude that Senior Associate may at least reveal Firm client's confidential information to Attorney in her consultation about a potential wrongful termination claim against her former Firm without violating Business and Professions Code, section 6068(e)(1) and rule 3-100(A). The facts state that the client confidential information is at the core of Senior Associate's wrongful discharge claim, so the gratuitous revelation of client confidences unrelated to any legitimate claim is not an issue. See *Dixon v. State Bar* (1982) 32 Cal.3d 728 [187 Cal.Rptr. 30]; San Diego County Bar Ethics Opinion 2008-1.

2. <u>Senior Associate may not publicly disclose Firm's client's confidential information to pursue her own claim.</u>

To what extent, however, may Senior Associate and Attorney use that information in pursuit of Senior Associate's claims? While Senior Associate may have the right to consult with Attorney—to get ethics advice or otherwise to determine her rights and responsibilities—neither *Fox Searchlight* nor *General Dynamics* addresses specifically how far Senior Associate and Attorney may go in using that information. May they use it in pleadings and open court?[3/]

In *General Dynamics, supra,* 7 Cal.4th 1164, the Court addressed two questions: (1) whether the in-house counsel's relationship with a former employer necessarily precluded a wrongful discharge retaliation claim against the former employer as a matter of law; and (2) whether and to what extent former in-house counsel could use client confidential information in the pursuit of that claim.[4/]

The Court concluded that, while nothing inherent in an attorney's role as in-house counsel precludes a retaliatory discharge claim, the attorney must establish the claim without breaching the attorney-client privilege or unduly endangering the values lying at the heart of the professional relationship. *Id*. at p. 1169.

> [T]he in-house attorney who publicly exposes the client's secrets will usually find no sanctuary in the courts. Except in those rare instances when *disclosure is explicitly permitted or mandated by an ethics code provision or statute,* it is never the business of the lawyer to disclose publicly the secrets of the client. In any event, where the elements of a wrongful discharge in violation of fundamental public policy claim cannot, for reasons peculiar to the particular case, be fully established without breaching the attorney-client privilege, the suit must be dismissed in the interest of preserving the privilege." 7 Cal.4th at p. 1190 (emphasis added).[5/]

General Dynamics permits retaliatory discharge remedies in instances where "*mandatory ethical norms* embodied in the Rules of Professional Conduct *collide with illegitimate demands of the employer* and the attorney insists on *adhering to his or her clear professional duty*." *Id.* at p. 1186 (emphasis in original). The *General Dynamics* Court cites being party to the commission of a crime, destroying evidence or suborning perjury as examples of such a "collision." Thus, *General Dynamics* would allow an in-house lawyer access to a judicial remedy (while concurrently prohibiting the public disclosure of client confidences in doing so) when fired for "adhering to the requirements of just such a mandatory professional duty, either by an *affirmative act* required by the ethical code or statute or by resisting a demand of the employer on the ground that it is unequivocally barred by the professional code." *Id*. at p. 1186 (emphasis in original).

In *Solin, supra*, Solin sued O'Melveny for alleged negligent legal advice given to Solin about Solin's clients. The *Solin* court had to decide whether to allow Solin's malpractice action against O'Melveny to proceed when

---

[3/] Although the California Evidence Code is implicated, our inquiry is focused on issues of professional responsibility and conduct.

[4/] *General Dynamics* reached the Court on a demurrer, General Dynamics having staked its defense on a client's unfettered right to discharge a lawyer for any reason or no reason at all. *Id.* at p. 1171. Unlike our facts here, in *General Dynamics*, the termination allegedly resulted from an in-house attorney's attempt to comply with his ethical obligations. See *id*. at p. 1169.

[5/] The court made clear that, in California, the ethical prescriptions at issue are those embodied in the Rules of Professional Conduct and certain provisions of the Business and Professions Code (e.g., §§ 6068, 6090.5-6107). *Id*. at p. 1190, fn. 6; see also *Green v. Ralee Engineering Co*. (1998) 19 Cal.4th 66, 78-79 [78 Cal.Rptr.2d 16].

O'Melveny contended that it needed testimony concerning the substance and details of discussions between Solin and the O'Melveny partner, including Solin's clients' secrets, and to introduce notes the O'Melveny partner took to corroborate his testimony. Since Solin would be duty bound (Evid. Code, § 955) to object to any evidence that revealed his clients' secrets, and since the trial court must exclude that evidence on a claim of privilege (Evid. Code, § 916), Solin would obtain an unfair advantage against O'Melveny. Accordingly, following the *General Dynamics* mandate if a lawsuit was "incapable of complete resolution without breaching the attorney-client privilege" (*General Dynamics, supra*, 7 Cal.4th at p. 1170), Solin's action could not proceed.[6/] *Solin, supra*, at p. 467.

In *McDermott, Will & Emery v. Superior Court* (2000) 83 Cal.App.4th 378, 385 [99 Cal.Rptr.2d 622], the court determined that the attorney-client privilege belonged to the corporation and refused to carve out a shareholder exception to that privilege even in a derivative action. The law firm would be unable to mount a defense in the shareholder derivative action, absent a waiver by the corporation, because it could not disclose the privileged communications that were alleged to constitute the breach of duty. As a consequence, the court directed the entry of judgment in the firm's favor.[7/]

Both *Solin* and *McDermott, Will & Emery* are consistent with *General Dynamics*' mandate that "where the elements of a wrongful discharge in violation of fundamental public policy claim cannot, for reasons peculiar to the particular case, be fully established without breaching the attorney-client privilege, the suit must be dismissed in the interest of preserving the privilege." 7 Cal.4th at p. 1190.[8/] But note that, in *Favila v. Katten Muchin Rosenman LLP* (2010) 188 Cal.App.4th 189 at p. 221 [115 Cal.Rptr.3d 274], the court concluded that a conditional stay, rather than dismissal, might be an appropriate remedy where there is a realistic possibility that the attorney-client privilege might be waived or an exception to the privilege may apply.[9/]

While no case directly addresses to what extent Senior Associate may *publicly* disclose client confidential information to the extent necessary to further her claims in a legal proceeding, in light of the absolute language in Business and Professions Code section 6068(e)(1), amended only to allow permissive disclosure in more dire

---

[6/] But see Evidence Code section 965.5 ["There is no privilege under this article if the lawyer reasonably believes that disclosure of any confidential communication relating to representation of a client is necessary to prevent a criminal act that the lawyer reasonably believes is likely to result in the death of, or substantial bodily harm to, an individual."]; see also Business and Professions Code section 6068(e)(2) and rule 3-100(B). The duty under Business and Professions Code section 6068(e)(1) is broader than the reach of the attorney-client privilege and covers "secrets" in addition to client confidences. *Goldstein v. Lees* (1975) 46 Cal.App.3d 614, 621 [120 Cal.Rptr. 253], fn. 5; State Bar Formal Opinions 2003-161 and 1993-133.

[7/] The court also rejected what it characterized as the "federal doctrine" with respect to the attorney-client privilege, holding that it contravened the strict principles in the Evidence Code that preclude any judicially-created exceptions to the privilege. (*McDermott*, *supra,* 83 Cal.App.4th at p. 385.)

[8/] The Court reiterated that "the contours of the statutory attorney-client privilege should continue to be strictly observed," rejecting any suggestion that the privilege should be diluted in the context of in-house counsel and corporate clients. "Matters involving the commission of a crime or a fraud or circumstances in which the attorney reasonably believes that disclosure is necessary to prevent the commission of a criminal act likely to result in death or substantial bodily harm, are statutory and well-recognized exceptions to the attorney-client privilege." *Id.* at p. 1191.

[9/] "It would be unfair to the derivative plaintiff and unnecessary to the preservation of the lawyer-client privilege to dismiss the lawsuit based on the *McDermott, Will* holding only to see the attorneys' client willingly waive its privilege to permit other defendants to defend themselves in the same lawsuit or to discover after such a dismissal that the evidence developed in the lawsuit against the allegedly culpable corporate insiders establishes the applicability of the crime-fraud exception of Evidence Code section 956." *Id.* at p. 221.

circumstances,[10] and the case law discussed above, we conclude that Senior Associate may not *publicly* disclose the Firm's client's confidences in order to pursue her own civil action.[11]

3. Attorney has a duty to Senior Associate to protect confidential information of Firm's client.

Attorney, unlike Senior Associate, has no prior or current relationship with the Firm or its clients. As a consequence, may Attorney disclose confidences of a Firm client that Senior Associate disclosed in seeking legal advice?

Attorney has two sets of duties to Senior Associate. First, Attorney is bound by the attorney-client privilege and Business and Professions Code section 6068(e)(1) to protect what Senior Associate reveals to him in consulting him about her potential claim against the Firm. As a consequence, unless Senior Associate can publicly disclose her former Firm's client's confidences, and only to the extent that she would be permitted to do so, Attorney is equally bound to protect those confidences from public disclosure because of his duty to protect the confidential information Senior Associate disclosed. (See Bus. & Prof. Code, § 6068(e)(1); rule 3-100.)[12]

Second, Attorney also owes Senior Associate a duty of competence under rule 3-110, not only to advance her interests but to avoid harming her. He is Senior Associate's agent and generally his conduct is imputed to her.[13] Thus, if Senior Associate cannot publicly disclose the Firm's client's confidential information, we conclude that Attorney is prohibited from engaging in such conduct.

CONCLUSION

While Senior Associate has the right to consult with Attorney concerning a potential wrongful discharge claim against her former Firm, and in that consultation to reveal, as necessary, client confidential information, in the circumstances described here, Attorney may not publicly disclose those client confidences to pursue Senior Associate's wrongful discharge claim.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Governors, any persons, or tribunals charged with regulatory responsibilities, or any member of the State Bar.

---

[10] An attorney is permitted to reveal confidential information only "to prevent a criminal act that the member reasonably believes is likely to result in death of, or substantial bodily harm to, an individual." Rule 3-100(B); *accord* Bus. & Prof. Code, § 6068(e)(2).

[11] We do not address whether the Firm's client confidences may be disclosed in some other manner (e.g., filing under seal, protective orders, or *in camera* proceedings). *See General Dynamics, supra,* 7 Cal.4th 1164 at p. 1191; *Favila, supra,* 188 Cal.App.4th at p. 221; San Diego County Bar Ethics Opinion 2008-1; *Solin, supra,* 89 Cal.App.4th at pp. 467-468; *Costco Wholesale Corp. v. Superior Court* (2009) 47 Cal.4th 725 [101 Cal.Rptr.3d 758] at pp. 737-739.

[12] See also Cal. State Bar Formal Opn. No. 1986-87; *Anderson v. Eaton* (1930) 211 Cal. 113, 116 [293 P. 788] (fidelity); *Jeffry v. Pounds* (1977) 67 Cal.App.3d 6, 11 [136 Cal.Rptr. 373] (loyalty); *In re Soale* (1916) 31 Cal.App. 144, 153 [159 P. 1065]; Cal. State Bar Formal Opn. No. 1996-146.

[13] *Channel Lumber Co., Inc. v. Porter Simon* (2000) 78 Cal.App.4th 1222, 1228 [93 Cal.Rptr.2d 482] (In a dispute between attorney and client, the court stated "a principal…may not employ an agent to do that which the principal cannot do personally.") See also, Cal. State Bar Formal Opn. No. 1995-144 (an attorney who directs investigator to interview witnesses to an accident must make sure that the investigator's communications with witnesses do not violate rule 1-400(A)) and Cal. State Bar Formal Opn. No. 1993-131 (a communication by client to opposing party that originates from the client's attorney is an indirect communication in violation of rule 2-100).

NOTES

26

Privacy and Security Developments in the Workplace (March 4, 2019)

Joseph J. Lazzarotti
Jackson Lewis P.C.

Rachel Roy
Sensata Technologies

Organizations continue to amass vast amounts of data from a myriad of sources and devices. They need this data to grow their businesses, service their customers, improve services to constituents, process payments, provide compensation and benefits to their employees, and a number of other everyday business functions. At the same time, the risks to that data continue to mount, regulation requiring the safeguarding of that data is expanding, and the challenges organizations and governments face to protect their data seem insurmountable.

Of course, virtually all organizations are employers, facing employee privacy and data security considerations are changing rapidly, almost daily, influenced heavily by the latest device, app, or social media platform. Employers are swimming in employee data, and new and more powerful devices and tools are available to capture and analyze that data. Simultaneously, workforces are increasingly mobile as employers are attracted by prospects for increased productivity, collaboration, and flexibility that technology can bring, but also burdened by the need to make critical company and customer data available to remote employees in an efficient and secure manner.

In some cases, employers encounter workplace issues that require an investigation – one employee accuses another of harassment, the organization's data loss prevention software alerts the company to a potential loss of sensitive data, a customer complains about an employee's activity in social media, or an employee is a consistently poor performer. No matter the reason for the investigation, information, sometime sensitive business and personal information, will need to be collected and examined by persons inside and potentially outside the organization.

When an investigation is warranted, a range of issues need to be considered, such as questions about the scope of the investigation, the information that needs to be collected and examined, the person(s) who will be conducting the investigation, who will have access to the information, and what happens to the data following the investigation regardless of its outcome. We discuss here some critical data privacy and security risks facing employers when carrying out investigations. We also help them to understand the kinds of steps they might want to take, and not take, to minimize those risks.

I. PRIVACY AND SECURITY LAWS AFFECTING INVESTIGATIONS

Employers want to maintain a respectful workplace, one in which good job performance does not shield wrongdoers from the consequences of

their actions. Whether seeking to enforce the organization's Code of Conduct or other policies and procedures, to manage performance, or to protect the organization, its assets, customers, or other employees, certain personnel in the organization need to undergo some level of information gathering to inform their decision making. Before hearing down that road, the employers needs to think about laws, regulations, and best practices that may affect the manner, extent, and nature of the information they collect, who has access to it, whether it can be accessed or transferred, how the information can be used, the safeguards needed to protect it, and how to handle the information at the conclusion of the investigation. Below are examples of some of the law, regulations and best practices that should be considered.

- **Information from Employee Monitoring Activities**. In addition to using video cameras to monitor employee activity, and monitoring employee telephone communications, employers are increasingly engaging in monitoring the activity and communications by employees on their information systems – e.g., websites visited, content of emails, files downloaded, and location of devices. When conducting an investigation, an organization's monitoring activities can be a fantastic source of information.

  Monitoring, in general, is permissible if carried out in a reasonable manner, for a legitimate purpose and consistent with employee expectations. Note also that in some states notice to employee is required for certain types of monitoring.[1] Of course, there are limits to monitoring. Connecticut law, for example, prohibits an employer from using "any electronic device to record or monitor employee activities in areas designated for health or personal comfort or for safeguarding of employee possessions, such as restrooms, locker rooms, or lounges." California, West Virginia, Rhode Island, Michigan and other states have similar laws prohibiting video cameras in bathrooms or locker rooms. Thus, before tapping these resources to inform an investigation, employers need to be sure that they have complied with applicable law, including giving notice where required.

  For example, monitoring employee communications, such as in company-provided email, an employer may discover communications between employees and their attorneys. Courts in most states have held that where an employer has a clear policy that alerts employees that its computer systems are monitored by the employer and that the employee does not have an expectation of privacy in the use of

1. See Delaware and Connecticut. Del. Code § 705, Conn. Gen. Stat. § 31-48d.

the systems, the employee has effectively waived the privilege. However, the New Jersey Supreme Court's decision in Stengart v. Loving Care rejected that view, citing the importance of the role that the privilege plays.[2] Thus, even if accessing the information was permissible, it may not be able to use the information as part of its investigation.

Employers also need to exercise care when accessing employees' e-mails during an investigation, particularly e-mails on personal e-mail accounts. In Pure Power Boot Camp Inc. v. Warrior Fitness Boot Camp LLC,[3] a non-compete case turned into a case about the privacy of stored e-mails and violations of the federal Stored Communications Act (SCA). The dispute arose when two employees of a fitness facility, Pure Power Boot Camp Inc., left to start their own fitness facility, Warrior Fitness Boot Camp LLC. A non-compete action followed because Pure Power learned through 546 mails it had accessed over a nine-day period that its former employees had taken customer lists, training and instruction materials, and solicited Pure Power customers. The e-mails were from four personal accounts belonging to the former employees' – Hotmail, Gmail, Warrior Fitness, and an unrelated corporate account. Pure Power was able to access these accounts because the former employees stored their usernames and passwords on its computers; when Pure Power accessed the particular site, the username and password automatically populated. The court ruled in the non-compete action that accessing the former employees' four accounts violated the SCA.

Employer also need to be aware of some unintended consequences of monitoring activities that may arise in an investigation. Under federal law[4] and in at least ten states[5] computer technicians or information technology workers must report child pornography if they encounter it in the scope of their work. The laws don't require technicians or service providers to search for the illegal material, only to report it if they find it. These laws are obviously not focused on employee privacy or data security or investigations. However, as

---

2. Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (2010).
3. *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, Llc*, 759 F. Supp. 2d 417 (S.D.N.Y. 2010).
4. 18 U.S. Code § 2258A.
5. http://www.ncsl.org/research/telecommunications-and-information-technology/child-pornography-reporting-requirements.aspx (Arkansas, California, Illinois, Missouri, North Carolina, Oklahoma, Oregon, South Carolina, South Dakota and Texas).

companies become increasingly more engaged in electronic monitoring activities, it is important to be aware of obligations like these.

- **Industry Regulation: HIPAA Privacy and Security Rules**. Employers and the persons who are charged with conducting investigations of employees need to be mindful of the regulatory environment facing the business, and how that may impact the information that they access and use in the investigation.

  The privacy and security regulations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") provided one of the first sets of comprehensive data privacy and security standards issued by a federal agency. The regulations apply only to certain types of health information, maintained by certain entities known as "covered entities"- health plans, health care providers, and health care clearinghouses. Although not specifically included in the list of "covered entities," many employers are, in effect, subject to the HIPAA rules. This is because, in general, they either (i) provide health care and transmit individually identifiable health information electronically in connection with certain covered transactions, or (ii) sponsor and administer covered health plans. This means, in part, that a HIPAA-covered hospital, for example, has HIPAA obligations with respect to its business of providing health care to patients, as well as with respect to the group health plan(s) that it sponsors for its employees.

  Over the years, there have been a number of changes to the HIPAA privacy and security regulations. The most recent is the changes made by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009, enacted as part of the American Recovery and Reinvestment Act of 2009 ("ARRA") which significantly expanded the types of entities to which HIPAA applies and how it is enforced, including extending enforcement authority to state Attorneys General. For example, many of the privacy and security standards that had been applicable only to covered entities, now apply to "business associates." Business associates could include, without limitation, claims administrators, insurance brokers, document shredding companies, software companies, a data storage/ cloud service providers, or law firms. Thus, when conducting an employment investigation that may involve protected health information, covered entities and business associates need to consider the HIPAA privacy and security regulations.

For example, a hospital employee may be accused of patient abuse. Investigating those accusations may require surveillance of patient interactions, examination of patient records, interviewing patients, and other activities that might result in the collection of protected health information about the patient. Before conducting this investigation, there are a number of privacy and security issues that needs to be considered, such as:

- Are the investigators collecting only the minimum necessary PHI to carry out the investigation?
- Who will have access to the information?
- Have these individuals been trained?
- If there are third parties assisting with the investigation, are they business associates and is there a business associate agreement in place?
- How will the information be stored during the investigation? Is it secure?
- Are there any more stringent state laws that have to be taken into account?

Whether it is HIPAA or some other framework of regulation that governs the management of data in a particular industry, when an investigation may involve data regulated by that framework, it needs to be factored into how the investigation is conducted.

- **GINA, ADA, and the FMLA**. To streamline the patchwork of federal and state laws intended to protect the public from genetic discrimination, Congress enacted the Genetic Information Nondiscrimination Act of 2008 ("GINA"), which prohibits discrimination on the basis of genetic information in employment and health insurance. Specifically, GINA prohibits workplace discrimination on the basis of genetic information through a combination of new laws and amendments to existing laws, including Title VII of the Civil Rights Act. GINA also adds provisions applicable to health insurance issuers and health plans concerning genetic information under the nondiscrimination and privacy provisions of HIPAA.

  With respect to employers, Title II of GINA prohibits discrimination on the basis of genetic information and restricts the acquisition and disclosure of genetic information. More specifically, Title II of GINA prohibits employers from making employment-related

decisions based on genetic information. Further, employers may not request, require, or purchase genetic information. Title II also requires that genetic information be maintained as a confidential medical record, and places strict limits on the disclosure of genetic information.

While GINA does have an inadvertent acquisition exception that applies when an employer acquires genetic information from documents that are commercially and publicly available for review or purchase (including newspapers, magazines, periodicals or books, or through electronic media, such as television, movies, or the internet), the exception does not apply to genetic information acquired by employers that access commercially and publicly available sources with the intent of obtaining genetic information. For example, an employer who acquires genetic information by conducting an internet search for the name of an employee and a particular genetic marker will not be protected by this exception, even if the information the employer ultimately obtained was from a source that is commercially and publicly available.

In addition to GINA, both the Americans with Disabilities Act ("ADA") and the Family and Medical Leave Act ("FMLA") require that employee medical records be kept confidential and not as part of the employee's personnel file. The FMLA requires that records and documents relating to medical certifications, re-certifications, and the medical histories of employees or employees' family members must be maintained as confidential medical records in files or records that are separate from personnel files.

For employers, handling employee medical records could be tricky, particularly in states such as California that have specific protections for that kind of information. Employers need to be able to identify when GINA, ADA, FLMA and state law protections apply and when they do not. They also need to be sure to safeguard the information appropriately, and when they are able to provide the information in response to a third party request.

Needless to say, employee medical information can be relevant to an investigation, or be obtained inadvertently. For the reasons stated above, employers need to proceed carefully when collecting and handling that information, as well as making decisions following an investigation based on that information.

When investigating claims concerning an employee's discriminatory activity on line in social media, an employer naturally may want to review the employee's activity and commentary. For reasons discussed elsewhere in this article, employers need to proceed

with extreme caution accessing private social media activity. However, even assuming the employer limits itself to only public statements made by the employee, it is possible that the employer may see posts concerning a disease that has manifested itself in one of the employee's family members, including the employee's spouse. Such information constitutes genetic information under GINA. The employer may have come across this information inadvertently, but any further use of it could expose the employer to liability under GINA.

The ADA also limits the handling of employee medical information which could inform the employer concerning who should be involved in the investigation and how the medical can be used and disclosed. For example, EEOC guidance[6] for healthcare employers provides:

> *19. Does the ADA require health care employers to keep applicant and employee medical information confidential?*
>
> Yes. Subject to several very narrow exceptions, all applicant and employee medical information, including written records and medical information provided orally, whether solicited by the employer or volunteered by the individual, must be kept confidential, and maintained in separate medical files rather than with personnel files. The employer may give medical information only:
>
> - to supervisors or managers in order to meet an employee's need for reasonable accommodation(s) or in connection with an employee's work restrictions;
> - to first aid or safety personnel where a condition might require emergency treatment or an employee would require assistance in the event of an emergency;
> - to government officials investigating compliance with the ADA or similar state and local laws;
> - as needed for workers' compensation purposes (for example, to process a claim); and,
> - for certain insurance purposes.

Based on the above, including managers and supervisors as part of an investigation in which they would have access to employee medical information of persons they supervise could raise compliance concerns under the ADA.

6. https://www.eeoc.gov/facts/health_care_workers.html.

- **Social Media Account Access Laws**. As noted above, it is not uncommon for managers and supervisors to use social media as a source in the course of an investigation. Many states have limited this practice, passing laws prohibiting employers from requesting or requiring employees to provide access to the employees' social media or online accounts.[7]

  However, a number these laws permit access in connection with certain investigations. The New Jersey law[8], for example, generally prohibits employers from requesting or requiring a current or prospective employee to provide or disclose any user name or password, or in any way provide the employer access to, a personal account. Also, under the law, an agreement to waive any right or protection is against the public policy of New Jersey and is void and unenforceable.

  However, the law permits employers to conduct investigations regarding: work-related employee misconduct based on information about activity on social media; or an employee's actions based on information about the unauthorized transfer of an employer's proprietary, confidential, or financial information to social media. Logically, the law also does not prevent an employer from viewing, accessing, or utilizing information about a current or prospective employee that can be obtained in the public domain.

  These kinds of exceptions are not identical across the states that have enacted these laws. Accordingly, companies need to educate those responsible for conducting investigations to consider these issues. A simple request could violate the law depending on the state. Thus, it is important to review the applicable state law carefully.

- **Credit Protection/Discrimination Laws**. Similar to the social media statutes above, a number of states have passed laws limiting whether and to what extent employers may access and use certain credit and similar information about employees. These laws are similar in concept but the language varies considerably and, therefore, they have to be reviewed carefully state to state. These states include Vermont, California, Colorado, Connecticut, Hawaii, Illinois, Maryland, Nevada, Oregon, Vermont and Washington. These laws generally seek to prevent discrimination against employees on the basis of poor credit, but also can be viewed as providing some level of privacy to an

---

7. http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx.
8. N.J. Stat. § 34:6B-6.

employee's personal finances. In those states, employers should take care with respect to the extent to which they take into account credit information of an employee they acquire in the course of the investigation. As noted, employers need to educate those running investigations about these requirements and direct them to handle such information in a permissible manner.

- **Constitutional and Common Law Privacy Protections**. Some states, like California, have constitutional privacy protections that extend to the private sector. In those cases, in the event the company is considering certain activity involving the searching or monitoring of employees, it should be sure to balance its legitimate purposes with the employees' expectation of privacy.

  Many states have common law torts concerning privacy which generally fall into four categories: (i) unlawful appropriation for a commercial purpose; (ii) publication of false, highly offensive information about a person; (iii) public disclosure of embarrassing private facts, and (iv) unreasonable intrusion upon one's seclusion. An example of activity that could trigger a claim under one or more of these torts is a company's deciding to conduct intrusive surveillance that runs outside the bounds of reasonableness. Despite how important the topic of an investigation may be, employers should consider how far their employees and contractors are going to find helpful information.

- **Affirmative Obligations to Protect Personal Information**. An increasing number of states require businesses to actively safeguard personal information (e.g., SSN, drivers' license number, financial account number including credit and debit card and back account information, medical information, biometric information) they own or maintain that belongs to residents of the state. The states that have enacted laws with these requirements include, without limitation, California, Connecticut, Colorado, Florida, Illinois, Massachusetts, Maryland, Oregon, and Texas. Note that Massachusetts likely has the most stringent law in terms of the detail provided for the kinds of safeguards that have to be put in place.[9]

  Compliance with these laws requires a number of steps, including without limitation, conducting and documenting a risk assessment

9. http://www.workplaceprivacyreport.com/2009/11/articles/written-information-security-program/the-final-final-massachusetts-data-security-regulations-and-a-checklist-for-compliance/ (regulatory checklist available).

(and updating those assessments periodically and as business changes dictate), establishing a data classification and access management policy, developing and implementing written administrative, physical and technical safeguards (aka a "written information security program" or a "WISP"), encryption, and training.

To provide more insight into the finds of safeguards that may be needed consider, for example, the guidance provided in February, 2016, by California's then Attorney General, Kamala D. Harris, now U.S. Senator from California, in her California Data Breach Report (Report)[10].

Perhaps the most consequential part of the Report for businesses is that it establishes a floor of controls that must be in place for a business to be considered to have adopted "reasonable safeguards" to protect personal information. Other states have a "reasonable safeguards" requirement, but have not provided further guidance concerning that standard. California's adoption of the Center for Internet Security's Critical Security Controls (The Controls) may provide multistate employers a path to achieving a greater comfort level in the protections they have (or need to have) in place for employment-related personal information.

Under California law, "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." [11] This requirement is important as the Report specifically states an organization's failure to implement all of the 20 controls set forth in the Center for Internet Security's Critical Security Controls (The Controls) **constitutes a lack of reasonable security**.

The Controls are set out in the table below:

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

10. *California Data Breach Report*, California Attorney General, Kamala D. Harris, February 2016. Available at https://oag.ca.gov/breachreport2016.
11. Cal. Civ. Code § 1798.81.5(b).

CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

The Report goes on to discuss numerous findings about breach types, data types, and industry sectors impacted. It concludes with five recommendations at stemming the tide of these breaches:

1. ***Reasonable Security***: Implement The Controls which are viewed by the State's Attorney General as a minimum level of information security.

2. ***Multi-Factor Authentication***. Organizations should make multi-factor authentication available on consumer-facing online accounts that contain sensitive personal information. This stronger procedure would provide greater protection than just the username-and-password combination for personal accounts such as online shopping accounts, health care websites and patient portals, and web-based email accounts. The same is true for employment-based portals.

3. ***Encryption of Data in Transit***. Organizations should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers.

4. ***Fraud Alerts***. Organizations should encourage individuals affected by a breach of Social Security numbers or driver's license numbers to place a fraud alert on their credit files and make this option very prominent in their breach notices. This measure is free, fast, and effective in preventing identity thieves from opening new credit accounts.

5. ***Harmonizing State Breach Laws***. State policy makers should collaborate to harmonize state breach laws on some key dimensions. Such an effort could reduce the compliance burden for companies, while preserving innovation, maintaining consumer protections, and retaining jurisdictional expertise.

Of course, in the course of an investigation, certain of the information protected by these statutes typically is not needed for the investigation, even if it is included in documents that are otherwise relevant. For example, a Social Security number (SSN) generally would not be relevant in a sexual harassment investigation. In fact, a number of states limit the situations in which businesses can acquire, use and disclose individuals' SSNs. For example, in Michigan and Connecticut[12], businesses need to maintain and publish a specific policy to address the SSNs they acquire. In Utah, employers cannot collect SSNs on the initial job application.[13] In New York, business should have policies to limit access to employee SSNs.[14] Because of how vital SSNs are to individuals and to the commission of

12. Mich. Comp. Laws § 445.82 *et seq.*; and Conn. Gen. Stat. § Sec. 42-471.
13. Utah Stat. Ann. § 34-46-201 *et seq*.
14. N.Y. Gen. Bus. Law §399-dd.

identity theft, it is critical that employers take steps to protect SSNs even if they do not have operations or employees in one of these states.

Thus, before sharing information concerning the investigation, consider whether it is prudent to redact such information. For example, when involving third party services providers to assist in an investigation, it may not be necessary to include SSNs in the materials provided to the service provider. If such information cannot be redacted, the information must consider whether "reasonable safeguards" are in place to protect that information.

- **Written Agreements With Service Providers to Safeguard Personal Information**. A number of states require companies that share personal information with third party service providers to obtain from such providers written assurances that they will safeguard that information. Some of these states include California, Maryland, Massachusetts and Oregon. At least with respect to data protected in these states, employees should be instructed not to share such information with vendors or allow vendors to access such personal information before an appropriate agreement is in place. Of course, it is prudent to apply this practice across the board when dealing with vendors, as well as with respect to all confidential data, and not just in the case of an investigation.

Depending on the circumstances, employers may want more robust protections for safeguarding personal information, and should consider including indemnity provisions concerning data breaches, procedures for handling data breaches and other protections, such as carrying appropriate data breach insurance. Developing a template data security addendum to be added to appropriate vendor contracts in the future can be particularly helpful to ensure acceptable provisions are consistently in place.

Some companies may want to go a step further and conduct vendor audits and assessments – to "kick the tires" by carrying out on-site assessments or data center reviews. More than putting contract provisions in place, as described above, taking a more proactive approach lets the vendor know the company is serious about data security.

Of course, part of the strategy for managing third party service providers in an investigation is to limit the information provided to them to the minimum necessary information to perform their serviced. This may not always be easy to determine. However, it should be

included as a regular step in the process so that it is top of mind as the investigation goes forward.

- **Breach Notification Statutes and Regulations**. All 50 states, as well as certain cities such as New York City and Washington D.C., require a business to provide notice when there has been a "breach" of "personal information" owned or licensed by the business.[15] While many of these statutes appear to apply to consumers, others such as the Massachusetts statute clearly apply to the personal information of employees.[16]

  During the course of an investigation, it is possible for data to be shared with unauthorized persons, lost, subject to a ransomware attack, or other circumstances that could constitute of breach of the security of the system maintaining such information. In that case, the employer must think carefully about whether it must notify the individuals who personal information was breached. Obviously, having to report the incident could derail the investigation and create additional exposure for the company. Accordingly, it is critical for the employer to provide guidelines to those involved in the investigation to be sure that information is protected and is used, shared, processed, and maintained in a secure manner. Thinking about this and other issues before commencement of the investigation can be crucial to avoiding a data breach, as well as prudently managing a data breach should one happen.

- **Data Destruction Mandates**. Over 30 states have enacted data destruction laws that require businesses to destroy records containing certain personal information by shredding, erasing, or using any other means to render the information unreadable or undecipherable.[17] A key step in an investigation is what happens at the conclusion of the investigation, when the information is no longer needed. Personal data in that case must be appropriately destroyed when it is being discarded. This includes selecting vendors that have strong protocols in place, are licensed where required (e.g., New York) and have appropriate certifications, such as through the National Association for Information Destruction.

---

15. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
16. Mass. Gen. Laws § 93H-1 et seq.
17. http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

- **International Laws: European Union's General Data Protection Regulation**

  Many U.S. organizations mistakenly think the European Union's data protection requirements do not apply to them. However, organizations that control or process the personal data of EU individuals may be subject to the General Data Protection Regulation (GDPR).[18] The GDPR imposes significant fines for companies that fail to comply. Penalties and fines, calculated based on the company's global annual turnover of preceding financial year, can reach up to 4% or €20 million (whichever is greater) for non-compliance with the GDPR, and 2% or €10 million (whichever is greater) for less important infringements. So, for example, if a company fails to report a breach to a data regulator within 72 hours, as required under Article 33 of the GDPR, it could pay a fine of the greater of 2% of its global revenue or €10 million.[19]

  While not all organizations in the U.S. will have GDPR-compliance requirements, many will and their executives and human resources, legal, and IT departments should be well-aware of their responsibilities. The HR department, for example, should be familiar with the provisions concerning human resources data, as well as those on employee monitoring and profiling or analytics activities. The GDPR's many privacy and security compliance requirements have undergone what is considered the greatest change to EU privacy and data security law in 20 years.

  Understanding GDPR and the laws in applicable countries can be critical for handling investigations which could involve individuals and their personal information from multiple countries. The effect and reach of GDPR is amplified because it how broadly it defined "personal data." Under the GDPR, "personal data" means information relating to an identified or identifiable natural person. A person can be identified from information such as name, ID number, location data, online identifier or other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[20] This even includes IP addresses, cookie strings, social media posts, online contacts and mobile device IDs.

18. https://gdpr-info.eu/.
19. https://gdpr-info.eu/art-33-gdpr/.
20. GDPR, Article 4.

Territorial Scope. A major change made by the GDPR is the territorial scope of the new law. The GDPR replaces the 1995 EU Data Protection Directive[21] which generally did not regulate businesses based outside the EU. However, now even if a US-based business has no employees or offices within the boundaries of the EU, the GDPR may still apply. Under Article 3 of the GDPR, an organization is subject to the new law if it processes personal data of an individual residing in the EU when the data is accessed.[22] This is the case where the processing relates to the offering of good or services or the monitoring of behavior that takes place in the EU.

Thus, the GDPR can apply even if no financial transaction occurs. For example, if your organization is a US company with an Internet presence, selling or marketing products over the Web, or even merely offering a marketing survey globally, you may be subject to the GDPR. That said, general global marketing does not usually apply. If you use Google Adwords and a French resident stumbles upon your webpage, the GDPR likely would not apply to the company solely on that basis. If, however, your website pursues EU residents – accepts the currency of an EU country, has a domain suffix for an EU country, offers shipping services to an EU country, provides translation in the language of an EU country, or markets in the language of an EU country, the GDPR will apply to your company. Likewise, if your company is engaged in monitoring the behavior of EU residents (e.g. tracking and collecting information about EU users to predict their online behavior), the GDPR likely will apply to your company.

However, if an investigation requires looking into issues that would include personal information of individuals in the EU, even if that investigation is being conducted in the U.S., critical issues need to be considered in advance of the investigation. One is whether the information can be transferred to the U.S., which GDPR regulators consider to have inadequate safeguards. Another issue is whether the information involved sensitive personal information that is subject to greater protections under GDPR and the law of the applicable EU member state. Thus, if an investigation is likely to reach personal data subject to the GDPR, a number of steps needs to be taken from a privacy perspective to ensure that the information can be transferred and considered in the course of the investigation.

21. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.
22. https://gdpr-info.eu/art-3-gdpr/.

Of course, the GDPR is not the only international law protecting personal data. When an investigation is likely to reach outside of the U.S., local law must be taking into account for shaping that investigation.

II. KEY STEPS TO CONSIDER CONCERNING PRIVACY AND SECURITY OF DATA COLLECTED IN INVESTIGATIONS

Workplace investigations are a necessary part of efficiently and effectively running a business. Because investigations can involve the collection of significant amounts of business and personal data, it is critical for the persons conducting the investigation to think carefully at all stages of the investigation, particularly at the beginning, about what information should be collected, who should have access to it, how is it safeguarded, what laws have to be complied with, how far can the investigation so, can we use the information and how, and what to do at the end of the investigation.

It is true that no amount of planning or system or set of safeguards is infallible. However, here are some basic steps employers can take to reduce the privacy and security risks inherent in many investigations. These steps are not exhaustive, but they are good starting points for discussion that can help shape a comprehensive and effective investigation procedure.

- **Plan Ahead**. Companies should have a high level outline and procedure for how it goes about conducting investigations. It should be clear who is responsible for commencing an investigation, shaping its direction, approving methodologies, carrying out the investigation, as well as who else may be involved in the process. (Of course, that may change based on the facts of the investigation, but some general guidelines can be helpful.) A written plan like this could aid those running the investigation to avoid missing privacy and security issues from the beginning, as well as other critical steps in the process. Indeed, privacy and security issues to consider will be peppered throughout the life of the investigation. Following any investigation, the company should revisit its plan to identify changes that would improve the process for future investigations.
- **Training**. From time to time, persons responsible for conducting investigations should run though the company's process for conducting investigation plan so they are familiar with the plan and issues such as privacy and security are top of mind, as well as knowing where the plan is.

- **Assess Capabilities in IT Team**. For many employers, it likely is easier to assess a salesperson's or even a chief executive's competence than the competence of the company's IT director. Often, management does not find this out until it is too late. The business should take steps to ensure it has the right team in this critical department.
- **Identify Third Party Service Providers**. Third party service provider could be critical to assisting the company with an emergent need for an investigation. Because the need for an investigation can arise suddenly, it is prudent to have vetted such third parties in advance, and come to general agreement on contract terms, including those terms concerning the handling of sensitive company and personal information. This would permit the company to get the process up and running more quickly.

Investigation can be a complicated and time-consuming process, one that leads to difficult decision. It is important that the requirements to protect critical data necessary for the investigation are not ignored. Data handled improperly could derail an otherwise successful investigation.

NOTES

NOTES

27

Alan Charles Raul and Stephen W. McInerney, Litigation Risks: How to Mitigate Litigation Risks Associated with Data Security and Cyber Defense (March 5, 2019)

Submitted by:
Alan Charles Raul
Sidley Austin LLP

GENERAL TYPES OF LITIGATION FOLLOWING DATA SECURITY INCIDENTS

- Regulator inquiries
    - Federal regulators – *e.g.*, FTC, HHS/OCR, SEC, CFTC, FCC, CFPB, banking agencies, DOJ, etc.
    - State attorneys general
    - Other state regulators – *e.g.*, NYDFS, insurance commissioners, NY AG Investor Protection Bureau
    - International data protection authorities, financial regulators, etc.
- Congressional inquiries
    - House Committee on Energy and Commerce
    - U.S. Senate Commerce Committee
- Consumer class actions – *e.g.*, victims of the cyber incident
- Federal securities litigation – *e.g.*, alleging damages driven by stock-price decline following the public disclosure of a cyber incident
- Shareholder derivative litigation – *e.g.*, alleging breach of fiduciary duties, corporate waste, insider selling, etc.
- International enforcement investigations and possible representative actions; Canadian class actions
- B2B litigation – *e.g.*, alleging breach of contract

CASE STUDY IN LITIGATION RISKS: EQUIFAX BREACH

- Equifax's historic data breach in 2017 impacted sensitive personal information of about 143 million people.
- "Hundreds of class actions" as disclosed in the 10-K.
- The litigation and regulatory fallout from the breach has been wide and far reaching:
    - FTC and CFPB are seeking legal remedy and fines.
    - NYDFS has warned the company that it may seek consumer relief and monetary penalties.

- Equifax faces a consolidated multidistrict consumer class action, multidistrict financial institution class action, and consolidated securities class action brought by investors.
- Lawsuit alleges three Equifax executives – including its CFO – sold almost $2 million worth of shares in the company, only days after the company learned of the breach but before the breach was publicly announced.

- 46-state and D.C. attorney investigation into the data breach.
- Suits by City of Chicago, City of San Francisco, Puerto Rico, Massachusetts, West Virginia.
- Multiple congressional inquiries, including the Senate Finance Committee and House Financial Services Committee.
- OPC in Canada and FCA in UK investigations.
- The Company has already received the maximum $125 million in insurance it had for cybersecurity incidents; meaning, the future breach-related losses will not be covered.
- TransUnion filed litigation alleging breach of contract.
- Securities and shareholder derivative litigation.
- Seven Canadian class actions.
- Etc., etc.

MITIGATION *BEFORE* A DATA SECURITY INCIDENT – ENHANCING LEGAL DEFENSIBILITY

A robust cybersecurity defense program provides a dual benefit: *first*, it decreases the chances of a data security incident occurring in the first instance; and, *second*, after an incident occurs, having had a strong cybersecurity defense program in plan before the incident helps the company demonstrate it took cybersecurity defense seriously and, the breach occurred despite the company's best efforts (and may even have been not reasonably avoidable).

- *General information security practices*
  - Conduct rigorous self-due-diligence, including a risk assessment that identifies foreseeable threats, vulnerabilities and uncovers and addresses red flags, land mines and unreasonable commitments or public statements.

- **Ex.** In December 2018, 12 state attorneys general filed a HIPAA breach lawsuit against Medical Information Engineering Inc. over a 2015 data breach that exposed data of 3.9 million individuals.[1] Among other things, the complaint alleged the Company's "information security policies were deficient and poorly documented" and that it had an "incomplete" incident response plan.[2]
- **Ex.** A 2018 class action lawsuit against Marriott alleges that the company failed to identify the breach and notify those affected in a timely manner. Plaintiffs allege Marriot should have discovered the breach during its acquisition of Starwood in 2016.[3]
- **Ex.** In the Equifax securities decision, the court highlighted a number of allegedly unreasonably positive public statements made by Equifax about its cybersecurity profile, such as: in SEC filings, Equifax stated that its success in safeguarding sensitive personal information was dependent upon its "reputation as a trusted steward of information"; Equifax's website provided that the company employed "strong data security and confidentiality standards" and maintained "a highly sophisticated data information network that includes advanced security, protections and redundancies."

- Ensure open communications between executives, lawyers and InfoSec teams.
  - **Ex**. In February 2018, the SEC made clear that a company's disclosure controls and procedures must ensure that information about cybersecurity risks and incidents is processed and reported to the appropriate personnel to enable senior management to make disclosure decisions and certifications.
  - **Ex**. The SEC settled with Yahoo! $35 million for allegedly failing to tell investors about a data breach for two

1. https://calendar.in.gov/site/oag/event/ag-curtis-hill-files-first-multistate-hipaa-related-data-breach-lawsuit/.
2. https://calendarmedia.blob.core.windows.net/assets/6771c02e-f4f1-4efd-b554-e419dc5bb898.pdf.
3. https://www.consumerreports.org/data-theft/class-action-lawsuits-against-marriott-data-breach/.

years. According to the SEC's release, "although information relating to the breach was reported to members of … senior management and legal department, [the company] failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors."

- Jina Choi, Director of the SEC's San Francisco Regional Office, said: The company's "failure to have controls and procedures in place to assess its cyber-disclosure obligations ended up leaving its investors totally in the dark about a massive data breach. Public companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to investors."

- Demonstrate rigor of compliance program document efforts to comply and train regarding legal/regulatory requirements, industry standards, and advisory opinions for information security (*e.g.*, NIST, SEC guidance, etc.) to counter arguments that you did not act reasonably or take reasonable measures to prevent a breach.
  - **Ex.** In the Equifax securities litigation, plaintiffs allege Equifax's data protection measures were "grossly inadequate," "failed to meet the most basic industry standards," and "ran afoul of the well-established mandates of applicable data protection laws."[4]
  - **Ex.** The SEC *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act* released on October 16, 2018 recommended that companies devise controls to ensure internal accounting controls reasonably safeguard the transfer of company funds.[5]
  - **Ex.** In November 2013, following a data breach at Adobe, a class-action lawsuit filed alleged in part that Adobe had under-invested in information security compared to its competitors.[6]

4. http://securities.stanford.edu/filings-documents/1063/EI00_15/2019128_r01x_17CV03463.pdf.
5. https://www.sec.gov/litigation/investreport/34-84429.pdf.
6. https://www.classlawgroup.com/adobe/.

- **Ex.** In a December 2014 lawsuit by multiple financial institutions against Home Depot, the plaintiffs alleged that the breach was "'the inevitable result' of Home Depot data-security practices 'characterized by neglect, incompetence and an overarching desire to minimize costs.'" They also claimed the retailer had ignored red flags, expert opinions, employee warnings and industry standards in its repeated refusal to upgrade security, and that their losses from the resulting fraud were in the billions.[7]

- Implement strong data hygiene practices.
  - Avoid collecting unneeded personal information;
    - **Ex**. Nationwide Insurance Co. agreed to pay $5.5 million in a settlement with 31 states and the District of Columbia following a 2012 incident wherein hackers allegedly exploited a known software vulnerability to gain access to the personal information of 1.2 million individuals. Many of the consumers whose data was allegedly lost as a result of the data breach were consumers who never became Nationwide's insureds, but the company retained their data in order to more easily be able to provide the consumers additional quotes at a later date.[8]
  - Require authentication and restrict access to company employees who have a specific business need to access sensitive information;
    - **Ex**. Connecticut led a nine-state settlement with TD Bank for $850,000 in 2014, following an incident where two backup tapes containing non-encrypted information on 260,000 customers were lost in transit.[9]

---

7. https://www.law360.com/articles/900084/home-depot-to-pay-25m-to-settle-banks-data-breach-claims.
8. https://portal.ct.gov/AG/Press-Releases-Archived/2017-Press-Releases/Conn-Leads-55M-Multistate-Settlement-with-Nationwide-Insurance-Company-over-2012-Data-Breach.
9. https://portal.ct.gov/AG/Press-Releases-Archived/2014-Press-Releases/AG-DCP-Announce-850000-Multistate-Settlement-with-TD-Bank-Over-Data-Breach.

        - Use industry-accepted methods to store and transmit sensitive information security; and
        - Consider deleting data after your use is complete.
    - Provide for open communication between technical experts and business units.
    - Require routine cyber training for employees to create a culture of cyber awareness.
    - Conduct ongoing vulnerability assessments.
- *Incident response plan*
    - Confirm your incident response plan is forward-thinking regarding post-breach litigation and regulator inquiries.
    - Ensure there are appropriate monitoring and reporting lines in place to detect breaches and alert senior management promptly once a breach has occurred.
    - Ensure the plan includes early involvement of attorneys and other advisers who can provide counsel about disclosure obligations.
    - Put in place procedures to institute stock sale holds to address insider trading issues.
    - Incident response team should meet on a regular basis, not just in response to an incident or threat.
    - Conduct table top exercises to test your incident response plan.
- *Internal audits and engagement of senior managment*
    - Establish a formal and documented internal audit program that is capable of effectively evaluating information technology controls.
    - Enhance oversight of IT operations as it relates to disaster recovery and business continuity functions.
    - Improve standards and controls for supporting the patch management function.
        - **Ex**. Plaintiffs in the Equifax securities litigation allege the company "manually" implemented its patching process across its entire network. This patching process "fell far

short" of industry standard, whereby peer companies used automatic patching processes.[10]

- Understand and evaluate company's cyber compliance culture.
- Judge whether Board and C-Suite are sufficiently involved.
- Receive comparison/benchmarking information regarding peers.
- Consider process or organizational refinements to enhance company's cyber compliance and defense posture.
- Review any communications with company's outside auditor regarding cyber.

- *Vendor management*
  - Improve oversight and documentation of its critical vendors.
    - **Ex**. On January 30, 2019, Aetna settled with the California Attorney General for $935,000 after Aetna (through a third party) used envelopes with an oversized clear window to send information to ~12,000 nationwide customers, thereby exposing information that the recipient was taking HIV-related medication.[11]
  - Ensure sufficient contractual protections for data and security – *e.g.* data protection agreements.
  - Audit external service providers.
- *Board oversight and management responsibility*
  - Improve management oversight of information security program.
    - Assess and analyze the impact of cybersecurity risks and incidents on a company's business.
      - Review cyber asset management process for identifying critical systems and information (*i.e.*, "crown jewels"), and setting priorities for commensurate safeguards.

10. http://securities.stanford.edu/filings-documents/1063/EI00_15/2019128_r01x_17CV03463.pdf.
11. https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-935000-settlement-aetna-over-allegations-it.

- All C-functions have some role to play, but there needs to be clear ownership.
- Devise and maintain controls and procedures to ensure timely regulator disclosures and filings regarding information security risks and incidents – *e.g.*, SEC disclosures.
  - Possible duty to correct or update prior cyber disclosures.
- Include cyber risk in M&A due diligence, reps and warranties.

○ Full Board should receive briefing at least annually on enterprise-wide cyber risk and cybersecurity investment.

- Reflect cybersecurity oversight in Board minutes.
- Avoid incautious phrasing of "risk acceptance" and business/security trade-offs.
- Don't just focus on PII risks; dig into potential operational impacts, business risks, and reputational or compliance implications (focus on SEC factors).
- Probe and understand any current significant pending or unresolved red flags.
- **Ex**. *Palkon v. Holmes* is a useful example where the board's actions helped defeat a shareholder derivative lawsuit against the directors and officers of Wyndham Worldwide Corp. following a series of data breaches. The court dismissed the case based on the business judgement rule—in part—because the board held 14 quarterly meetings in which it discussed the cyberattacks and company security policies and proposed security enhancements, as well as the board appointed the audit committee to investigate the breaches, and that committee met at least 16 times to review cybersecurity.
- **Ex**. As part of Home Depot 2017 settlement of a shareholder derivative action following a data breach, the Company agreed to certain policy reforms including maintaining an executive committee focused on data security and requiring regular reports on information technology budget and spending on cybersecurity.

- *Regulatory filings and public statements*
    - Ensure pre-breach statements of cybersecurity defense and internal controls are accurate and comprehensive.
        - Such statements can include:
            - SEC filings – *e.g.*, 10-Q, 10-K, 8-K, publicly filed stock purchase agreements, etc.
                - SEC Guidance published in February 2018 clarified expectations regarding the quality and usefulness of cybersecurity disclosure, and the compliance and governance framework with respect to how cybersecurity risks and incidents are handled.
                - **Ex**. Equifax's 10-Ks for 2015[12] and 2016[13] described the credit monitoring service as "delivering security" and touted Equifax's development of "new technology to enhance the . . . security of the services we offer." These statements became the basis for plaintiffs' complaint alleging Equifax made "false and/or misleading" statements about its cybersecurity vulnerabilities.
            - Website – *e.g.*, privacy policy
                - **Ex**. Plaintiffs in the Equifax securities litigation pointed to statements on the company's website as evidence of the company's allegedly false statements regarding cybersecurity: Equifax's website provided that the company employed "strong data security and confidentiality standards" and maintained "a highly sophisticated data information network that

12. https://otp.tools.investis.com/clients/us/equifax/SEC/sec-outline.aspx?FilingId=10515045&Cik=0000033185&PaperOnly=0&HasOriginal=1.
13. https://otp.tools.investis.com/clients/us/equifax/SEC/sec-outline.aspx?FilingId=11207464&Cik=0000033185&PaperOnly=0&HasOriginal=1.

includes advanced security, protections and redundancies."[14]

- Investor conferences
- SOX certifications

▪ Avoid definitive statements—such as "the Company has never been a victim of a successful hack"—as there may be breaches that the Company is not aware of.

▪ Ensure statements include appropriate caveats—*e.g.* do not say "our cybersecurity defense is fully consistent with best practices in our industry."

- **Ex**. In denying Equifax's motion to dismiss in part, the Court looked to "aspirational" statements regarding cybersecurity defense: Equifax allegedly repeatedly stated that "cybersecurity, an important aspect of their business, was a top priority for senior management, despite the fact that Equifax failed to employ some of the most elementary cybersecurity practices."[15]

○ Ensure statements regarding compliance with data privacy laws are accurate, especially in light of the GDPR and the CCPA.

▪ **Ex**. In August 2018, after missing their earnings targets, an investor claimed Nielsen Holdings PLC allegedly misled stockholders about how Europe's privacy overhaul would affect the company's access to Facebook data and other information for analytics business in a proposed class action in New York federal court.[16]

- *Cybersecurity Legal Governance Assessment*

○ Consider conducting a pre-incident "Cybersecurity Legal Governance Assessment" – a rigorous internal self-diligence to find and fix landmines.

---

14. http://securities.stanford.edu/filings-documents/1063/EI00_15/2019128_r01x_17CV03463.pdf.
15. http://securities.stanford.edu/filings-documents/1063/EI00_15/2019128_r01x_17CV03463.pdf.
16. https://www.law360.com/articles/1076082/nielsen-hit-with-shareholder-suit-over-eu-privacy-impacts.

- Objectives include:
  - to enable Board, CEO and GC to address company's cybersecurity governance, legal posture and defensibility on cyber risks; and
  - to obtain internally focused due diligence and legal advice to help detect, prevent and defend against significant compliance problems, regulatory investigations and foreseeable claims; prepare to manage potential major cyber crises.
- Some cybersecurity issues to probe include:
  - Understand responsibilities, organization, spending, reporting and accountability for cybersecurity program
  - Review information security and incident response programs
  - Understand and decide whether and how company applies NIST Cybersecurity Framework
  - Understand whether company applies or is subject to any other external standards (e.g., ISO, PCI, FFIEC, etc.)
  - Review insider threat program and experience
  - Review results of existing penetration tests, and ongoing process
  - Review company's history of incidents, handling of incident response and legal claims (and analogous situations for relevant peers)
  - Review processes to identify, track, log and resolve "red flags"
  - Review, evaluate and assure adequacy of budget, staffing, resources and support from management
  - Understand significant perceived risks, weaknesses, significant "unsuccessful" attacks, and serious fears of InfoSec team

MITIGATION *AFTER* A DATA SECURITY INCIDENT

The steps a company takes after discovering a data security incident has occurred are critical to mitigating the risk of litigation or regulatory

inquiry. Proper execution of the company's incident response plan—and thoughtful, decisive decisions during the response—will put the company in the best position to defend against any subsequent legal actions.

- *Follow your incident response plan*
    - Alert proper stakeholders in a timely manner to ensure the scope of the breach is known, and limit any further damage.
        - **Ex**. In December 2018, 12 state attorneys general filed a HIPAA breach lawsuit against Medical Information Engineering Inc. over a 2015 data breach that allegedly exposed data of 3.9 million individuals. Among other things, the complaint alleged that, while the Company was investigating the malware attack, the attackers were still able to exfiltrate further data through SQL queries – demonstrating that the company's post-breach response was "inadequate and ineffective."[17]
        - **Ex**. Massachusetts Attorney General settled with Yapstone Holdings for $155,000 in December 2018 for a data breach allegedly involving personal information of 6,800 Massachusetts residents. Allegedly, a Yapstone employee learned of a vulnerability on its website in August 2014, but the company neglected to fix it until August 2015 (when another employee learned of the vulnerability).[18]
    - Properly investigate the incident.
        - **Ex**. In April 2018, Yahoo! paid a $35 million fine to settle SEC claims that the company allegedly misled investors by failing to disclose a "massive" cybersecurity breach. The SEC alleged "Although information relating to the breach was reported to members of Yahoo's senior management and legal department, Yahoo failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors."[19]

17. https://calendarmedia.blob.core.windows.net/assets/6771c02e-f4f1-4efd-b554-e419dc5bb898.pdf.
18. https://www.mass.gov/news/payment-processor-to-pay-155000-over-data-breach-affecting-thousands-of-massachusetts.
19. https://www.law.com/therecorder/2018/10/23/yahoo-agrees-to-pay-85m-to-settle-consumer-dat-breach-class-actions/.

        - **Ex**. In September 2018, the Massachusetts Attorney General settled with UMass Memorial Medical Group and UMass Memorial Medical Center for $230,000 following two separate incidents where former employees allegedly inappropriately accessed patient information, which was subsequently used in identity theft and fraud crimes. The Attorney General's lawsuit alleged the hospitals "knew of these employees' misconduct but failed to properly investigate complaints related to these breaches, discipline the employees involved in a timely manner."[20]
    - Communicate with appropriate senior management and the board of directors.
    - Initiate stock holds, if necessary.
        - **Ex**. Lawsuit alleges three Equifax executives, including its CFO, sold almost $2 million worth of shares in the company only days after the company learned of the breach but before the breach was publicly announced.[21]
        - **Ex**. Yahoo Inc, Intel Corp., and PayPal Holdings Inc. have also been hit with cyber-related securities fraud claims over the past few years.[22]
    - Consider notifying law enforcement.
    - Review contractual agreements to determine notification requirements.
- *Notify regulators and consumers within the appropriate timeline.*
    - Each state differs with regard to what constitutes a data breach, how PII is defined, and the timing for notification to state regulators and affected individuals.
        - States attorneys general are very active in this space, and routinely fine companies for delayed notification.
        - **Ex**. In October 2017, the New York and Vermont attorneys general jointly settled with Hilton for $700,000 total

20. https://www.careersinfosecurity.com/massachusetts-hipaa-case-outlines-series-missteps-a-11551.
21. https://www.npr.org/sections/thetwo-way/2017/09/08/549434187/3-equifax-executives-sold-stock-days-after-hack-that-wasnt-disclosed-for-a-month.
22. https://www.law360.com/articles/1019321/the-rise-of-cyber-related-securities-fraud-class-actions.

following a data breach involving 350,000 customer credit cards. Hilton first learned of the breach in February 2015, and a second breach in July 2015, but did not notify affected customers until November 2015.[23]

- Certain federal regulators may also require notification following data breaches – *e.g.*, SEC.

- **Ex**. In April 2018, Yahoo agreed to pay $35 million to resolve SEC claims that it allegedly failed to notify investors for two years about its 2014 breach.[24] *Ensure public statements and filings are accurate.*
  - Duty to disclose cyberattack in public filings or statements – *e.g.*, SEC filings, earnings calls, etc.
    - Steven Peikin, co-director of the SEC enforcement division, explained: "We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But …."[25]
  - Disclosures regarding the risk of potential *future* cyberattacks and their attendant harms may be materially misleading without incorporating discussion of known cyberattacks.

- *Perform a postmortem.*
  - Identify additional ways to improve your company uses of information technology, and act on your findings.
  - Revisit incident response plan, if necessary.
  - Document that you have learned lessons from your prior incidents and analogous incidents within the relevant industry as well as other major public incidents.

23. https://ag.ny.gov/press-release/ag-schneiderman-announces-700000-joint-settlement-hilton-after-data-breach-exposed.
24. https://money.cnn.com/2018/04/24/technology/yahoo-altaba-hack-sec-fine/index.html.
25. https://www.sec.gov/news/press-release/2018-71.

NOTES

NOTES

28

Tips from the Trenches to Make Your Company Less Attractive to Cyber Enforcement

Aimee Nolan

W.W. Grainger, Inc.

Jason N. Smolanoff

Kroll, a division of Duff & Phelps

Antony Kim

Orrick Herrington & Sutcliffe LLP

Aimee Nolan is Vice President, Associate General Counsel and Chief Intellectual Property Counsel at W.W. Grainger, Inc. Jason Smolanoff is a former FBI Supervisory Special Agent, and currently is a Senior Managing Director, Global Cyber Rick Practice Leader at Kroll. Antony (Tony) Kim is a partner and co-founder of Orrick, Herrington & Sutcliffe LLP's Cyber, Privacy & Data Innovation Practice.

Proactive risk management is a dynamic, multi-faceted opportunity for companies of all sizes. In the cyber realm, the core issue is typically around calibrating investments in security to align with properly identified threats and vulnerabilities. This requires a holistic view drawn from key stakeholders across departments and disciplines. It also warrants tough debate on enterprise priorities and resources. Companies rarely get it 100% right. But they enhance their chances of doing so through structures and processes that account for the critical interplay between Governance (input and accountability), Operations (practical business considerations and capabilities), and Controls (technical, physical and administrative) – in that order.

At the end of the day, the goal is clear: to appropriately assess and mitigate risk to the enterprise and its key stakeholders. Unfortunately, that risk increasingly includes the potential for enforcement by a regulatory agency and/or the plaintiffs' bar. Nearly every U.S. state and federal agency has cyber at the top of its agenda. And statutes such as the California Consumer Privacy Act of 2018[2] portend a next-generation of laws that will inject *statutory* breach damages into the mix – ostensibly eliminating the need to show any actual harm to consumers, similar to other statutes with unbalanced punitive consequences like the TCPA.[3] Substantial fines and penalties, brand and reputational damage, and a host of other liabilities, including for directors and officers, are squarely on the table for the foreseeable future.

Against this backdrop, there is no "easy button" to push. But there are certainly some easy wins. And while there is no such thing as perfect security, there are some steps that make perfect sense. Our hope is that shared, common experiences and insight might help *lawyers* to positively influence the management and mitigation of cyber risk. In that regard, this article offers some lessons learned from the trenches in the form of seven actions that can help your company down the road.

---

2. The CCPA provides that any consumer whose non-encrypted or non-redacted personal information is subject to unauthorized access and exfiltration, theft or disclosure due to security failures on the company's part can sue "to recover damages in an amount not less than $100 and not greater than $750 per incident or actual damages, whichever is greater." Cal. Civ. Code § 1798.100, *et seq.*
3. The Telephone Consumer Protection Act (TCPA) provides a private right of action for "actual monetary loss from such a violation [or] $500 in damages for each such violation, whichever is greater." 47 U.S.C. § 227(b)(3) (also providing for trebling of damages if a court finds willful or knowing violations).

1. KEEP GOOD COMPANY

It has never been more important to diligently vet, onboard, monitor and audit critical third-party service providers and vendors. These third parties exist to make life easier, more efficient and more innovative and to help you better service your customers. To do so, they often have access to, ingest and store tremendous amounts of data for various processing purposes. Given this reality, it is hardly surprising that vendor-attributed data breaches are increasingly common. A recent study by Soha Systems found that 63 percent of data breaches may be directly or indirectly related to third-party access by contractors and suppliers.[4] And while there are certainly examples of bad press and enforcement activity against a service provider who suffers a data breach, by far, the rule is that the company bears the brunt of its service provider's cyber-mistakes and mishaps. Continued corporate migration to the cloud, and the growth in outsourcing generally, set the stage for significant third-party risk going forward.

On this front, the Securities and Exchange Commission's 2018 cyber guidance is instructive.[5] Throughout the guidance, the Commission repeatedly cites to third-party "suppliers," "service providers," and "vendors" as critical to, among other things, enterprise risk, cyber incidents, and potential breach response and remediation costs. Companies are admonished to think long and hard about how service providers might be discussed in their public filings (e.g., "Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure."). Indeed, the fallout from a third-party breach can be significant for companies that have tight operational connectivity and integration with their vendors (e.g., in the supply chain). Where companies rely on third parties not only for operational support but also for cybersecurity controls, the stakes may be even much higher. The same goes for companies who rely on service providers to provide critical e-commerce support. In these scenarios, a failure in the vendor's measures designed to protect against, identify, detect, or respond to major cyber events could materially impact the company.

Despite these warning signs, many organizations still struggle to get their arms around their service providers. A 2018 Ponemon study[6] found

4. Soha Systems, "Third Party Access Is A Major Source of Data Breaches, Yet Not An IT Priority," (April 2016) (online survey of over 219 IT and Security C-Level Executives, Directors and Managers).
5. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 CFR 229, 249 (2018).
6. Ponemon Institute, "Data Risk in the Third Party Ecosystem" (Nov. 2018).

that 59% of survey respondents reported experiencing a data breach caused by a third party. That number increased 5% from 2017, and up 12% from 2016. More than 75% of respondents believe that third-party data breaches are increasing. But nearly one quarter of respondents admitted that they *did not know* if they had had a third-party breach in the past 12 months. More troubling is that only 35% of respondents are confident that a third-party vendor would notify them if the vendor suffers a data breach. And only 11% are confident that a downstream fourth-party vendor would notify them of a breach.

Much has been written about the design and execution of robust vendor management programs. We do not wish to duplicate that here. It goes without saying that vendor management can impose significant costs, and we are not advocating the outsourcing of vendor management to yet another service provider (e.g., companies that offer website/online scanning technology). Rather, we offer three tips on less notorious, but (in our experience) effective risk mitigation moves that counsel might consider vis-à-vis third parties:

- Define "Breach" Strategically, Address Cooperation, and Seek a No-Past-Breach Rep: In the U.S., the scope of notifiable data breaches is actually quite narrow as only certain types of data and certain circumstances trigger mandatory notification regimes. In vendor contracts, companies should consider what types of cyber security events or incidents matter in terms of managing their risk, and negotiate for definitions consistent therewith. Moreover, in our experience, companies and their vendors must cooperate with each other when a cybersecurity incident occurs that affects them both. When third-party breaches happen, regulators not only look at the security commitments that a company obtained from the vendor, but also the speed and quality of information and cooperation that the company obtains from the vendor to can help to more quickly and effectively mitigate harm to any impacted consumers. Finally, we have found that it can be very helpful to include a draft contractual rep that the vendor is not aware of facts or circumstances suggesting a past "breach" (defined, as discussed above). This type of rep has two benefits. First, it usually prompts a discussion with the vendor around different types of incidents that the vendor has experienced, and whether or not they are covered by the rep. Second, because many breaches trace back to hacks and other events that occurred many months or even years ago, a no-past-breach rep can provide significant leverage should the rep turn out to be untrue.

- When Bargaining Power is Unequal, Implement Compensating Controls: In many situations, a service provider is so large, powerful and essential, that companies are unable to negotiate for customized contractual protections. In these situations, counsel are well advised to work with their clients to identify and implement compensating controls. This can be as simple as turning on a multi-factor authentication option that the vendor offers, or as complex as implementing supplemental encryption strategies.
- Exercise Your Audit Rights: In our experience, when regulators investigate a breach attributable to a service provider, the fact that the company had a contractual *right* to audit compliance, is becoming less and less acceptable. Regulators want to see more. Counsel should take time to identify critical vendors and to the extent no audit process is in place, consider the possibility of some (any) checks on whether vendors are living up to their security commitments. And as regulatory requirements and expectations evolve, they should be reflected in both vendor management practices as well as in updated contractual provisions.

2. DIG BEFORE YOUR GET HITCHED

While vendor relationships are important, it gets "real" when your company contemplates a merger, acquisition, joint venture, or major partnership deal. Recall that Verizon cut $350 million off Yahoo!'s price tag after the latter revealed three breaches involving 3 billion accounts. It was a defining event in cyber history. And it continues to serve as a poignant reminder to all companies – buyers and sellers; large and small; public and private – about the criticality of robust cyber diligence. It is literally true that a company can *buy* a cyber incident that subsequently exposes it to potentially substantial liability. Marriott's 2018 disclosure of a Starwood breach that allegedly began in 2014 (prior to Marriott's acquisition of Starwood) proves this unfortunate point.

According to a 2016 New York Stock Exchange and Veracode survey,[7] 22% of directors said that they would *not* acquire a company that had experienced a high-profile data breach. Nearly half of respondents in a 2016 Brunswick Insight survey[8] said that they would discount a target's valuation based on a data breach – whether the breach was discovered

7. NYSE/Veracode, *Cybersecurity and the M&A Due Diligence Process*, Survey Report (2016).
8. Brunswick Insight, *Brunswick Data Valuation Survey,* 3rd Annual Survey (2016).

before, during or after the transaction. More recent studies suggest that while more cyber diligence is being performed, it may be resulting in less deals. According to a 2018 study by West Monroe Partners,[9] which analyzed survey findings over the past three years: a greater percentage of dealmakers are discovering a cybersecurity problem at the target only *after a deal has closed* – up from 40% finding post-deal problems in 2016 to 58% in 2018; nearly half of corporate buyers are dissatisfied with cybersecurity due diligence – up from 3% dissatisfied in 2016 to 49% in 2018; and executives are citing cyber-related red flags as among the top reasons for abandoning a deal.

It is important to note that comprehensive soup-to-nuts diligence is often impractical and unrealistic. M&A transactions, for example, typically involve multiple suitors competing for the same target. Compromises and concessions are part of negotiating a complex deal. Timeframes are tight. Resources are limited. It is also exceedingly difficult to find an opening, or willingness, to perform the type of technical penetration tests and compromise assessments, and compliance reviews, that a buyer might otherwise pursue.

As with vendor management, the publicly available guidance on cyber diligence is plentiful. That guidance draws from diverse viewpoints, including but not limited to banking, consulting, accounting, legal, government and academia. Here, we offer a few insights from the buyer's perspective that, in our experience, have helped to get at the heart of the issue:

- Non-Public Cyber Incidents: Because most cyber-attacks and data breaches do not trigger mandatory notification rules, as with the vendor discussion above, it is important to understand whether the target has experienced broadly-defined data "incidents" (e.g., ransomware, DDOS, data corruption/loss, theft of proprietary information or trade secrets) and the associated remediation strategy and results. Equally important is assessing any history of non-compliance fines or penalties that are not public, such as those involving the card brands and PCI.
- Validating Publicly Made Representations: As discussed further below, what a company publicly says about cybersecurity in its Privacy Policy, Terms of Use, or even marketing materials, is classic fodder for regulator and class action complaints. Opposing parties point to allegedly "deceptive" statements that customers and consumers

9. West Monroe Partners, *Cybersecurity Issues in M&A Continue to Grow,* White Paper (2018).

relied on to their detriment. These are low hanging fruit for enforcement cases and can be challenging to defend.

- Reverse Vendor Management: Where the target is a service provider/vendor, the buyer should assess whether and how the target anticipates and addresses (including through contractual protections) its own customers' compliance requirements. This is particularly important where the target's customer base or data-types are highly regulated – e.g., financial services; healthcare; defense contracting; PCI/payment card data; children's data: data subject to prescriptive rules such as the EU's General Data Protection Regulation (GDPR).

3. THOUGHTFULLY DEPLOY PRIVILEGE

Legal counsel's role in cybersecurity has evolved significantly over the past 10-15 years. While lawyers traditionally were called in to reactively handle lawsuits and regulatory actions, they now contribute to shaping proactive cyber planning, assessment and resiliency efforts, including incident response.

Apart from their legal knowledge, lawyers have always provided clients a safe place for hard debate and even harder decision-making. The American Bar Association explains that the "underlying purpose" of the attorney client privilege is "to encourage persons to seek legal advice freely and to communicate candidly during consultations with their attorneys without fear that the information will be revealed to others." It is also well established that disclosures of information to experts/consultants who are necessary for a lawyer to render legal advice to a client, do not waive the privilege.

In the cyber context too, the case law strongly supports privilege (and attorney work product) protections over consultants engaged by counsel *in the aftermath of a data breach*. For example, in early 2015, the District Court for the Middle District of Tennessee denied Visa's discovery requests relating to materials produced by two security firms that Genesco's counsel engaged to, respectively, (i) investigate alleged past violations of PCI DSS, and (ii) assist in efforts to comply with PCI DSS. The court ruled that both sets of materials were protected, holding that "attorneys' factual investigations fall comfortably within the protection of the attorney-client privilege," and privilege "extends to [third-party forensic consultants] that assisted counsel in its investigation."[10] Similarly, in

10. *Genesco, Inc. v. Visa USA, Inc.,* No. 3:13-cv-00202 (M.D. Tenn. Mar. 25, 2015).

late 2015, the U.S. District Court for the District of Minnesota rejected class plaintiffs' move to obtain core investigative materials and communications from an internal "Data Breach Task Force" and third-party consultant Verizon – both of which were engaged and directed by Target's lawyers following the retailer's high profile breach in 2013.[11] The court upheld Target's privilege and work product assertions for all materials related to its "dual track" investigation, except for a few documents that reflected CEO updates to Target's Board of Directors.[12]

With respect to *proactive (non-breach) cyber risk assessments*, a recent February 2019 decision from the Premera Blue Cross breach litigation[13] provides critical insights into how courts are likely to address privilege assertions. The Premera case stems from a data breach disclosed in 2015. Class actions were filed and discovery battles ensued. The court considered a broad range of document categories set forth in Premera's privilege log, the highlights included analyses of privilege assertions over security audits and assessments. In this regard, the court noted as follows:

> Regarding Premera's audits and investigations of their information technology and security, Premera's general information technology and training . . . the Court is *not persuaded that these were primarily done with legal purpose and not business purpose*."

Observing that "[a]s a business, Premera needs periodically to audit its information technology and security and training," the court stated that the audits "would have happened regardless of any pending litigation or regulatory investigations." The court was particularly skeptical of two audits that occurred years before Premera's breach, referring to such audits as simply "normal business functions." And while Premera claimed that its counsel was involved in the audits, the court flatly remarked that "Premera cannot shield them from discovery by delegating their supervision to counsel."

The fact that case law is now developing on the issue of cyber-related privilege, makes clear that lawyers are increasingly playing a meaningful role in this space. However, there are some key lessons learned that are food for thought for both in-house and outside lawyers:

---

11. *In re Target Corporation Customer Data Security Breach Litigation,* No. 14-2522 (D. Minn. Oct. 23, 2015).
12. *See also In re Experian Data Breach Litigation,* No. 15-01592 (C.D. Cal. May 18, 2017) (reports created by Mandiant consultants retained by outside counsel deemed to be attorney work product).
13. *In re Premera Blue Cross Cust. Data Sec. Breach Litig.,* 2019 WL 464963 (D. Or. Feb. 6, 2019).

- Non-Breach Cybersecurity Audits or Assessments: Counsel should carefully manage client expectations and differentiate between audits or assessments that are routine "normal business functions" versus those that are truly directed by counsel for purposes of rendering legal advice. Proactive (pre-breach) work always involve tradeoffs between remediation and resources (i.e., tough choices are made about what to do now versus put-off until later). Debates like these can generate prejudicial documents. Counsel should seek to shield them from potential discovery to the extent they are properly subject to the privilege.
- Deploy Privilege Through "Drafts": Even if a cyber audit or assessment might not qualify for attorney client privilege or work product protections, there are strategies to shield the debate and decision-making from disclosure. For example, emails to counsel that discuss the pros/cons of an audit, items to investigate or focus on, tradeoffs and compromises, priorities and key risks are legitimately privileged. In addition, as the Premera court recognized, "[a] draft report sent to counsel seeking legal advice and input on the draft also would be privileged." Another practice is to conduct oral read-outs before things are reduced to writing.
- Engaging Public Relations (PR) Firms: The typical incident response playbook contemplates PR/crises communications teams being engaged through counsel for privilege purposes. However, there is mixed case law on this point. For example, some courts have distinguished between "standard" public relations services aimed at preserving a public image or reputation versus PR firm communications or work product that are directly related to legal advice or litigation strategy.[14]

4. TAKE YOUR COMMUNICATIONS TEAM TO LUNCH

In the wake of a data breach, companies must navigate a host of legal, risk and reputational landmines. However, perhaps nothing influences liability – and drives the appetite of public and private enforcers – more

14. *Compare McNamee v. Clemens* (E.D.N.Y. 2013) (no privilege; PR firm only provided standard services not necessary in order to provide legal advice, and therefore disclosing documents to firm resulted in waiver) *and King Drug Co. v. Cephalon, Inc.* (E.D. Pa. 2013) (privilege applied; consultants preparing business and marketing plans were the client's "functional equivalent").

than the first *external communication* that a company makes about a cyber incident.

For example, offering credit monitoring and identity protection services in the wake of breach has become standard playbook practice. Indeed, consumers and employees often expect these types of services, regardless of the nature or scope of the information that was compromised. This can create tension between legal counsel who are concerned about litigation risk, and business/communications professionals who want to protect brand loyalty and demonstrate the company's commitment to customers or employees.

Interestingly, the mere offering of these services may send an unintended signal, for example where the breach does not involve Social Security Numbers or other data used for identity theft (e.g., medical information). In that situation, a company may face questions such as: "Was more data compromised than the company reported?" or "Does the company have evidence of identity theft attributable to the breach?" or "Are consumers at real risk of identity theft?" This is not to say the scales should tip in favor of foregoing a credit monitoring remedy. However, a string of cases over the past several years should prompt lawyers to spend more time with their corporate communication colleagues.

- In upholding the plaintiffs' standing to sue, the Seventh Circuit in *Neiman Marcus*[15] specifically cited to the company's offer of one year of credit monitoring and ID theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. According to the court, it was "unlikely that it did so because the risk is so ephemeral that it can safely be disregarded," noting that "these credit monitoring services come at a price that is more than de minimis." In other words, the court effectively used Neiman Marcus' decision to broadly offer free credit monitoring as a concession that plaintiffs faced non-speculative and imminent risk of harm, warranting their mitigation expenses.
- In the *P.F. Chang's*[16] case, the Seventh Circuit likewise pointed to what it described as an "implicit" admission that compromised card data could be used to open new cards because P.F. Chang's "encouraged consumers to monitor their credit reports (in part for new-account activity) rather than simply the statements for existing affected cards."

15. *Remijas v. Neiman Marcus Group LLC,* 794 F.3d 688 (7th Cir. 2015).
16. *Lewert v. P.F. Chang's China Bistro, Inc.,* 819 F.3d 963 (7th Cir. 2016).

Thus, the company's cautionary reminder to monitor credit reports—a statement that many states statutorily require companies to include in breach notifications—rendered the plaintiffs' purchase of credit monitoring service and efforts to guard against ID theft, reasonable mitigation expenses sufficient for standing purposes.

- In *Nationwide Mutual Insurance*,[17] the Sixth Circuit relied, in part, on Nationwide's offer to provide credit monitoring as evidence of the reasonableness of mitigation expenses for standing purposes. But the court further noted that Nationwide had recommended that consumers consider putting a freeze on credit reports, explaining that such freezes could impede the ability to obtain credit, and could cost a fee between $5 and $20 to place and remove such freezes. Notwithstanding that some states require companies to advise consumers about the availability of a credit freeze (e.g., Massachusetts), the Sixth Circuit pointed to Nationwide's credit freeze advice, the associated costs, and Nationwide's failure to offer coverage for those costs, in ruling for the plaintiffs.

This is not to say that lawyers should ring the alarm bells on post-breach notifications. Rather, in our experience, early brainstorming, sharing of case law (such as the cases mentioned above), and coordination can help to reduce the risk that breach notifications catch company stakeholders by surprise when they are later quoted in legal briefs and court orders. In addition, we offer the following lessons learned that can be included in every lawyer's next discussion (hopefully over lunch) with her communications colleagues:

- Early Announcements Can Be Risky: The above cases serve as a cautionary tale for making public announcements regarding a security incident before the internal and forensic investigation is complete. To the extent that reputational and other considerations (e.g., leaks) demand early communications, organizations should be very careful in disseminating information too broadly (e.g., sending an e-mail alert to all employees about a potential security incident) or in over-disclosing to external stakeholders.
- One-Size-May-Not-Fit-All For Precautionary Messages: It is critical to understand the nuances of the state-specific notification requirements. Many states (including Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia and Wyoming) explicitly require that

17. *Galaria v. Natiowide Mutual Insurance Co.,* 663 Fed. Appx. 384 (6th Cir. 2016).

the reporting company include specific recommendations to consumers on risk mitigation, including encouragement to monitor credit reports. However, notwithstanding variations across state rules, a commonly accepted practice is for organizations to issue a standard notification that complies with substantially all of the states' various requirements (except Massachusetts), and supplement certain notifications based on state-specific requirements (e.g., instructions on contacting a specified state agency/regulator). This means that all of the various state-required language and disclosures are often provided to all individuals, even if not entirely applicable. Although they often reflect sound security practices that consumers should follow in any circumstance, organizations should recognize the risk in making risk mitigation recommendations, and consider whether to provide them only to consumers whose states' law explicitly requires it.

- Carefully Describe Protective Measures: Certain state statutes require disclosure of the measures taken to contain, mitigate or minimize the incident. For example, Michigan directs that notifications "generally describe what the [company] providing the notice has done to protect data from further security breaches." Wyoming requires a description in general terms of "the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches." Similar requirements exist in North Carolina, Vermont, Virginia and elsewhere. However, these types of statements have been used to infer the scope of individuals who were affected. Thus, although statutorily required, these cases demonstrate why organizations should thoughtfully articulate the containment/remedial measures taken in response to an incident.
- Rigorously Analyze Voluntary Notifications: In our experience, even if a cyber incident does not technically trigger a notification requirement, companies often "voluntary" notify affected parties. They do for a host of different reasons. We see counsel's role as helping stakeholders to assess the pros/cons of voluntary notification through decision trees that account for downside and upside (e.g., the likelihood that voluntary notice will enable customers to take meaningful self-help steps).

5. DON'T FORGET ABOUT PRIVACY

A few years ago, the Federal Trade Commission wrote a blog post that highlighted key issues companies should expect to be asked about in cyber investigations. Among other things, the FTC explained that the agency looks at "privacy policies and any other promises the company has made to consumers about its security."[18] Indeed, most FTC cyber enforcement cases turn on allegations that a company made misleading statements regarding the type, strength, or even presence of, security measures associated with its product or services. Offending statements can appear in a variety of contexts, including privacy policies, terms of service, marketing materials, and even investor relations materials, just to name a few.

In this vein, the Third Circuit's landmark decision in *FTC v. Wyndham Worldwide Corporation*[19] is instructive. On three occasions in 2008 and 2009, hackers allegedly ex-filtrated payment card data of over 619,000 of Wyndham's guests. The FTC brought an enforcement action under the unfairness prong of Section 5 of the FTC Act, arguing that Wyndham's security practices "unreasonably and unnecessarily" exposed personal data to unauthorized access and theft. The complaint also raised a deception claim for allegedly misleading statements in the company's privacy policies. Those policies contained allegedly false representations that data was protected according to "industry standard practices" and "commercially reasonable efforts," such as using "128-bit encryption," "fire walls" and "other appropriate safeguards."

Although the FTC's deception claim was *not* on appeal, Wyndham's privacy policy emerged as a critical factor in the decision upholding the unfairness claim. The court noted that a company does not act equitably when it "publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business." Moreover, "consumers could not reasonably avoid injury by booking with another hotel chain because Wyndham had published a misleading privacy policy that overstated its cybersecurity." Finding it plausible that consumers were misled by Wyndham's privacy policy, the court deemed the policy "directly relevant" to whether the company's conduct was "unfair."

---

18. M. Eichorn, "If the FTC comes to call," Blog Post, *available at,* https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call (May 25, 2015).
19. *FTC v. Wyndham Worldwide Corporation,* 799 F.3d 236 (3d Cir. 2015).

Private plaintiffs routinely allege that companies not only fail to protect data (thereby resulting in a breach) but deceive consumers in privacy policies with security-related misrepresentations. For example, these types of allegations featured heavily in complaints against Marriott following its 2018 announcement that Starwood databases had been breached starting in 2014 (e.g., "Ultimately, Marriott could and should have prevented the data breach by implementing and maintaining reasonable safeguards, consistent with the representations Marriott made to the public in its marketing materials and privacy statements, and compliant with industry standards, best practices, and the requirements of [] State law. Unfortunately, Marriott failed to do so, and as a result, exposed the personal and sensitive data of hundreds of millions of consumers.")[20]

We offer the following tips for identifying potential privacy-related cyber exposure points:

- Check What Your Company Publicly States About Security: Be thoughtful about the fine line between transparency that informs customers on the ways in which you collect, use, share, store and transfer data, and vague language or catch phrases, such as "industry standard security," "bank-level encryption" or "we do everything we can do to secure your data" that can land a company in hot water. Decide whether detailed statements about your plans, protocols, processes and tools are necessary and generate any value. Avoid overstating your security practices, or implying that a high level of security is applied across the board, if in fact it is applied is more limited circumstances (e.g., subsets of data; data in-transit versus at-rest; applied by the company but unknown for service providers).
- Regularly Refresh Assessments of Publicly Made Statements: All external (consumer) facing representations should be reviewed no less than twice per year. Reviews should be accelerated as part of privacy-by-design processes any time new products or services will be deployed. Counsel should conduct these reviews as group exercises with mandatory participation by IT/InfoSec and Marketing/e-commerce (who often have first line-of-sight to new tools and technology being considered and deployed).
- Consider Reasonable Security Disclaimers: We regularly see privacy policies that trumpet claims like "Security Guaranteed" and "Bank Level Security" (often by non-financial services entities!). Given the

20. Complaint, *Hiteshew v. Marriott International Inc., et al.,* No. 8:18-cv-03755 (D. Md. Dec. 6, 2018).

shifting cyber threat landscape, virtually any assurance regarding security is susceptible to legitimate scrutiny. This is why many companies include blanket disclaimers that security measures may change, be unavailable from time to time, or even circumvented by sophisticated actors (e.g., "We cannot guarantee 100% security. No security is fail proof"). Competent judgment is required to strike a thoughtful balance: any legal benefits that disclaimer language may provide should be weighed against the PR/business impact of being viewed as shifting risk to the consumer. And even though disclaimers are not a panacea, they can at least provide arguments regarding what consumers should reasonably expect.

6. MIND YOUR DIRECTORS AND OFFICERS

In-house counsel, and outside counsel who work with them, technically represent the company. They are fiduciaries to the corporate entity, which has as its highest authority, the Board of Directors. Accordingly, an important part of the general counsel's role is to provide sound legal compliance and legal risk mitigation advice to the Board.

While it is a new risk, cybersecurity falls squarely within the traditional "risk oversight" obligations of corporate Directors. Directors have fiduciary duties to act in good faith, and with care and loyalty, which, in the cyber context, includes directing Management to design, implement and enforce a robust cybersecurity compliance program. To effectively do so, Directors must be educated and informed about the company's risk profile, threat actors, and strategies to address that risk; they must receive regular briefings from Management and metrics to understand progress toward the desired state.

Indeed, the Securities and Exchange Commission recently emphasized the criticality of the Board's cyber activities to the marketplace.[21] In its 2018 cyber guidance, the SEC stated that disclosure in annual reports or proxy statements of the board's role in risk oversight of a company pursuant to Item 407(h) of Regulation S-K *should* include a discussion of the nature of the board's role in overseeing the management of cybersecurity risks that are material to a company's business. In addition, the SEC observed that disclosures on how the board engages with management on cybersecurity issues will allow investors to assess how a board of directors is discharging its risk oversight responsibility in cybersecurity matters.

21. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 CFR 229, 249 (2018).

The foregoing is not surprising given the potential severity that breaches can have on a company's performance and value, including its brand and reputational assets. That has spurred shareholder derivative suits against directors and officers in the aftermath of major data breaches. In these suits, plaintiffs allege that the directors and officers failed to ensure effective cybersecurity programs, recklessly ignored security warnings and various red flags, and, as a result, the company had inadequate controls and procedures to protect personal and financial information against unauthorized access and acquisition.

We offer three insights from the frontlines of governance work that we believe has the dual benefit of not only helping to mitigate risk for the company, but also helping directors and officers to fulfill their cyber-fiduciary duties:

- Practice with Your InfoSec Team: While cyber risk is not "new," its high level of Board attention is certainly new. InfoSec teams, often for the very first time, are in the Board room, and responsible for educating the Board on the company's risk profile, vulnerabilities, current security state, and roadmap for remediation and sustained risk management. Accordingly, they need practice and guidance from counsel (e.g., regulatory and litigation perspectives) to be most effective in communicating with the Board. Counsel's early involvement is particularly important when the Board will assume a more active role – for example, where InfoSec conducts a Board-level incident response tabletop, or discusses ransomware attacks and the issue of who in the company decides whether to pay.
- Vertically Integrate InfoSec with the Governance/Disclosures Team: From a governance perspective, many companies do not involve their InfoSec teams in the risk disclosures process and committee. Especially for public companies, lawyers can help to establish a channel for reporting cyber events, and the appropriate Board committee (whether the Audit, Risk, of even Cybersecurity Committee) can thereby gain experience around assessing events for disclosure filing purposes
- Implement Trading Blackout Protocol for Cyber Events: Based on the 2018 SEC cyber guidance, lawyers should assess whether procedures are in place to determine whether implementing a trading blackout period while the company investigates and assesses the significance of a cyber incident is appropriate, and review insider

trading policies to ensure they prohibit insiders from trading when in possession of material nonpublic information relating to cyber risks or incidents.

7. ASSESS YOUR RISK ASSESSMENTS

Cyber risk assessments come in dozens of flavors. They can involve enterprise or product level analyses, focus on people, processes, or technology (or all three), be limited to certain systems or all of them, and relate to the company or its service providers (or both). But what *all* risk assessments have in common is that they identify lots of "opportunities" for improvement. For that reason, both regulators and private plaintiffs demand them in discovery. The absence of a risk assessment can be a red flag *and* the presence of unaddressed recommendations arising out of risk assessments can form the basis for alleged liability in a data breach or even a security-vulnerability case.[22]

For legal counsel, risk assessments are relevant and useful in a number of respects. For example, risk assessments can play a key role in helping to evaluate the vendor management program, as well as helping to assess the vendors' own security programs. They can also be leveraged to evaluate cyber or privacy issues related to an acquisition target; or leveraged by a target company to ready itself for acquisition or other major transaction (or even a cyber insurance underwriting). Risk assessments can also be used to benchmark a company's overall security program or elements of its (e.g., incident response) against regulatory requirements, industry standards/best practices, or customer requirements. In some cases, an enforcement agency may request a risk assessment in the aftermath of a breach, or as part of a settlement. Having a recent assessment already done in the ordinary course can go a long way in demonstrating diligence and mitigating regulatory scrutiny.

As with any audit or assessment, the challenge for companies is prioritizing and executing on the remediation plan. While some companies have robust processes for identifying corrective actions, road-maps, milestones, and funding requirements, many companies struggle – and thereby, unintentionally create an unfavorable paper trail and precedent.

---

22. The FTC has exercised its prosecutorial discretion to investigate and bring actions against companies for security vulnerabilities even in the absence of any data breach. *See, e.g.,* Complaint, *FTC v. D-Link Corporation*, No. 3:17-cv-00039 (N. D. Cal. Jan. 5, 2017).

This last point was driven home in the Financial Industry Regulatory Authority's (FINRA) investigation and consent order against Sterne Agee in 2015.[23] Sterne Agree is a registered broker dealer based in Alabama. The company found itself embroiled in one of FINRA's very few cyber enforcement actions, largely due to the following fact pattern:

- In May 2014, an employee inadvertently left a laptop with personal data related to over 350,000 consumers in a public restroom, and it was stolen. The laptop was not encrypted.
- Previously, as early as March 2009, the company recognized the need for laptop encryption but considered it a "moderate risk" due to a low laptop count. As the number of laptops grew, the associated risk of not implementing encryption also grew.
- By 2010, the company had approved the purchase of Microsoft's BitLocker encryption software.
- In 2010 and 2011, BitLocker was not installed on any laptops because the company needed additional IT personnel. Funding for those personnel was not approved until 2012.
- In 2012, when the newly hired personnel attempted to install BitLocker, it was found to be incompatible with the company's laptops.
- Employee turnover subsequently delayed the company's identification of a compatible encryption solution, but funding for the solution was not approved until June 2014 – *after* the unencrypted laptop was stolen.

The Sterne Agee case is an extreme example of a simple proposition familiar to every lawyer: repeated identification of the same risk can expose the company to potential liability. This proposition has made its way into regulator actions and class action complaints. For example, the FTC has explained that in cyber investigations, the agency requests and reviews "materials like audits or risk assessments that the company or its service providers have performed."[24] On the class action side, plaintiffs in the Equifax breach litigation alleged that the company failed to remediate known security deficiencies, and repeatedly ignored warnings from third-party consultants. One Senator summarized her findings on this point following congressional hearings and investigative activities:"

23. FINRA Letter of Acceptance, Waiver and Consent, Sterne, Agee & Leach, Inc. (Respondent), No. 2014041619501 (May 22, 2015).
24. M. Eichorn, "If the FTC comes to call," Blog Post, *available at,* https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call (May 25, 2015).

> Equifax was warned of the vulnerability in the web application software Apache Struts that was used to breach its system, and emailed staff to tell them to fix the vulnerability – but then failed to confirm that the fixes were made. . . .
>
> Equifax received a specific warning from the Department of Homeland Security about the precise vulnerability that hackers took advantage of to breach the company's systems . . . and several outside experts identified and reported weaknesses in Equifax's cyber defenses before the breach occurred. But the company failed to heed – or was unable to effectively heed – these warnings.[25]

While it is certainly easy for outsiders to critique in hindsight, the tone and tenor of the allegations clearly set forth a roadmap for identifying key exposure points. We offer three thoughts on how lawyers might leverage cyber assessments to help proactively manage enterprise risk:

- Focus on Repeat Items: Lawyers should hone in on documented weaknesses, warnings and action items that continue to show up from audit to audit or assessment to assessment, particularly those that map to non-compliance with a specific law, regulation, or contractual requirement (e.g., PCI). Depending on their criticality and remedial potential (e.g., if fixes are reasonably available), these repeat items can form the basis for serious regulatory and private liability – particularly if any even arguably contribute to a future data breach. Of course, context is always relevant to assessing liability exposure. For example, remediation recommendations must be viewed in the context of whether the risk item was deemed "accepted risk" by the company; the probability of the risk event occurring is also relevant; and counsel should probe whether compensating controls exist to mitigate the risk item's criticality for prioritization purposes.
- Deploy Privilege Via Emails and "Drafts": As discussed above, risk assessments are a double-edged sword – helping to *identify* security risks while simultaneously *creating* remediation risks for the enterprise. Thus, it bears repeating that even if a cyber audit or assessment might not qualify for privilege or work product protections, there are strategies to shield legitimate debate and decision-making. Lawyers should be consulted *precisely* in situations where tradeoffs must be made between remediation and resources – as these choices often carry significant legal compliance, regulatory and litigation risk repercussions. Drafts of reports sent to counsel for legal advice, as well as

25. "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information," Prepared by the Office of Senator Warren (Feb. 2018), *available at,* http://www.warren.senate.gov (last accessed Feb. 27, 2019).

emails and conversations that occur outside the four corners of an assessment, are almost always covered by the attorney client privilege.

- Focus on Assessments That Are Tightly Linked to Strict Legal Requirements: In our experience, risk assessments produce broad recommendations that cover a lot of ground, including actions that range from necessary to advisable to nice-to-have. Counsel should work with business and security teams to develop a defined schedule on the corporate calendar for conducting risk assessments in areas like HIPAA and PCI that produce specific, targeted remediation recommendations. In addition to being able to identify specific issues, there is value in being able to demonstrate a culture of compliance should the company experience a public breach or regulator investigation.

* * *

Cyber risk is constantly evolving, and intensifying the enforcement risk that companies face from both regulators and private litigants. As lawyers are increasingly involved in proactive risk management, our hope is that at least some of the "easier" wins discussed in this article allow counsel to add value to the process. Of course, there is never enough time, enough money or people to do everything. But prioritized, targeted work holds the best potential for mitigating cyber risk for the enterprise and its stakeholders.

NOTES

29

Considerations for Data-Rich Contracting Post-GDPR

Flora J. Garcia

McAfee, LLC

Disclaimer: This was prepared for and is intended as general guidance for use in the 2019 PLI Institute on Privacy and Data Security Law Conference, San Francisco, CA. These statements, opinions, and any errors are my own and not those of my employer. The statements and this article do not constitute legal advice, and each company must determine for itself its obligations under all laws. Nothing herein establishes an attorney client relationship.

For privacy professionals the world over, the General Data Protection Regulation ("GDPR")[1] rapidly and intensely changed many things. The goal of unifying the myriad European Economic Area country laws regarding privacy since the European Union's Data Protection Directive ("Directive")[2] was inevitably an ambitious and massive undertaking.

In the year after the GDPR's enforcement date of May 25, 2018, the questions around the meaning of the GDPR have only grown in number. The GDPR changed many things and has explicit and prescriptive requirements for agreements between data controllers and data processors. While many of the constructs and requirements in the GDPR existed under prior laws and the Directive, the relative lack of enforcement has allowed for broad interpretations of what constitutes mandatory compliance. While likely required when transferring data outside countries providing adequate protection under the Directive, under the Regulation a Data Processing Agreement (or similar binding document) containing specific and prescribed language is mandatory between entities where the personal data of European Economic Area residents is being handled, even if it does not leave the residents' home country or the EEA. Additionally, the European Banking Authority has issued Recommendations on Outsourcing to Cloud Service Providers, which despite their name are binding on financial services providers in the EEA as of July 1, 2018.[3] Additionally, the European Banking Authority (EBA) published on February 15, 2019 its revised Guidelines on outsourcing arrangements setting out specific provisions for the governance frameworks of all financial institutions within the scope of the EBA's mandate with regard to their outsourcing arrangements and related supervisory expectations and processes. The aim of the Guidelines is to establish a more harmonized framework for these financial institutions, namely credit institutions and investment firms subject to the Capital Requirements Directive (CRD), as well as payment and electronic money

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2. Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.
3. See https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf/e02bef01-3e00-4d81-b549-4981a8fb2f1e for the Recommendations and "EBA issues guidance for the use of cloud service providers by financial institutions" at https://eba.europa.eu/-/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions for an overview (both last visited March 5, 2019).

institutions. The recommendation on outsourcing to cloud service providers, published in December 2017, has also been integrated into the Guidelines.[4] The California Consumer Protection Act (CCPA or CaCPA), while not explicitly addressing contractual expectations, requires companies to reveal other companies to which they pass (and especially sell) personal data on California residents.[5]

The goal of this piece is to offer a non-exhaustive checklist for considering data protection in agreements from a variety of points of view. The hope is that such a checklist will start discussions around risk appetite, the distribution of risk between the parties, and customary fallback positions. The goal of this piece is to provide a framework for considering the activities contemplated under an agreement, rather than to offer specific provisions or clauses. Plenty has been written about what to include within a Data Processing Agreement (or a Data Protection Agreement or Data Transfer Agreement),[6] but consideration of these concepts should assist in constructing a holistic approach to the risks under the GDPR and successor laws that evolve from it and the Directive, including other similarly organized laws in other countries.

KEEP A HISTORICAL CONTEXT[7]

In thinking about data protection laws, it is always important to pause a minute and consider the historical underpinnings of much of the body of law within which we currently operate. For many of us, the Data Protection Directive has been in play for much of our careers, but it was not the first privacy or data protection law by far. In 1970, centuries ago for those of us working in the internet economy, the state of Hessen in Germany passed the first data protection law amid fears of a return of the misuses of personal data that took place when the Nazis used early data

4. https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements.
5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199], see https://iapp.org/resources/article/california-consumer-privacy-act-of-2018/ (last visited March 5, 2019).
6. Additionally, many companies are now making these documents public. See, for example, Cisco's Supplier Privacy and Information Security Exhibit at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/supplier-privacy-information-security-exhibit.pdf and IBM's Data Processing Addendum https://www.ibm.com/support/customer/pdf/dpa_en.pdf (both last visited March 5, 2019).
7. Some of this section relies on Flora J. Garcia, Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators, 15 Fordham Intell. Prop. Media & Ent. L.J. 1205 (2005).

sorting devices to establish Jewish ancestry.[8] In 1973, Sweden's Data Act became the first national privacy law.[9] Calls from the European Parliament for the European Commission to propose a directive harmonizing early laws came as early as 1976; Norway, Austria, Germany, Sweden, France and the United Kingdom all had blocked or prohibited data flows to at least one other country by 1990.[10] The Directive was formally adopted on October 24, 1995, and, as a Directive requiring Member state transcription into local laws, was to have been implemented by the states within three years. In January 2000, the European Commission took legal action against member states (France, Luxembourg, the Netherlands, Germany, and Ireland) that did not pass national laws to incorporate the data protection elements of the Directive as required. An important aspect of the Directive was the obligation on each member state to establish a "public authority" or agency to administer the Directive's requirements[11].

Unlike a directive, which requires the transcription of the Member states into their own laws, a Regulation under EU law is immediately enforceable, as is the GDPR adopted in May 2016, with an enforcement date of May 25, 2018, at which time the Directive was no longer in force. Though a major aim of the GDPR is to normalize the Member State laws, the GDPR still allows for some 57 topical variances (known as Derogations), which if taken advantage of and executed differently in even some of the Member states can create a significant new morass of requirements.

THE WORDS WE USE: DEFINITIONAL MATTERS

The holder of the fundamental human right of privacy is the "data subject" under EU law, and under the GDPR, there is a definition of what data exactly should be considered in scope. Article 4 of the GDPR offers the following definition:

> "'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one

8. David Scheer, *For Your Eyes Only: Europe's New High-Tech Role: Playing Privacy Cop to the World*, WALL ST. J., Oct. 10, 2003, at A1.
9. Eduardo Ustaran, ed., European Data Protection Law and Practice (2018).
10. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 199 n.16 (1992).
11. For a much more comprehensive review of how we got here, please consult the IAPP's European Data Protection Law and Practice, edited by Eduardo Ustaran (*op. cit. 5*), and see especially the timeline and list of other European data protection and privacy laws in Section 1.7.2.

> or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"[12]

Note carefully the inclusion of online identifier or location data as an element of personal data. Consider the possibility that, under the GDPR, we are seeing a radical shift from a binary perception of what is and is not personal data to a sliding volume control, in line with the requirements for considering the risk of harm related to the types of data.

Additionally, the GDPR and longstanding data protection law uses the terms data controller and data processor to describe the roles of the corporate, organizational, or governmental entities handling the personal data:

> "'[C]ontroller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;[13]
>
> '[P]rocessor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"[14]

Processing is often used synonymously with "use," but it will be important to note its definition in the GDPR as well:

> "'[P]rocessing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"[15]

So basically, any access to personal data can be interpreted as a processing activity.

A YEAR LATER, STILL RIFE WITH UNCERTAINTY

Some of the consternation in preparations for the GDPR enforcement date were a result of aspects of the law where there has been little guidance or definition. But even as we have seen the first of the GDPR fines (at the time of this writing: an Austrian betting pub's CCTV recorded too much public space; Knuddels, a German social media platform reported a data breach, but was fined not for the breach but for storing passwords in

12. GDPR Article 4 (1).
13. GDPR Article 4 (7).
14. GDPR Article 4 (8).
15. GDPR Article 4 (2).

plaintext; a Portuguese Hospital allowed too much access to patient records; and Google fined from France for a lack of transparency and consent), we have little to assist us in the complexity of transactional work. in those areas in which we have guidance from the member state data protection regulators and/or the Article 29 Working Group or its replacement group, the European Data Protection Board, we do not have a crystal ball that will show us how fines will be enforced and exactly how the regulators and the courts will interact in applying the GDPR. It well may be more than a decade before we have clarity, and, as is the case with any laws focused on technological advancement, it is likely that the state of the art will have outpaced the regulatory and judicial process. While uncertainty comes with an economic cost, it will benefit negotiators, transactional attorneys, and privacy professionals to keep in mind that at the core of the GDPR, as well as at the core of any data protection laws stemming from Europe, is the importance of privacy as a fundamental human right, and that at least one of the major drivers for the Directive and the GDPR has been to remind businesses – especially those not established in the European Union – of their obligations to the individuals whose data they hold and use.

One of the difficulties for the Directive and the associated member state laws that arose under it was that the threat of actions for noncompliance was not generally painful to large, multinational corporations. The focus on member state by member state actions, as opposed to a pan-EEA or EU action, tended to make the number of records or impacted data subjects smaller. With the advent of the GDPR's maximum fines of 4% of annual worldwide turnover (revenue in U.S. parlance) or $20 million Euro, whichever is higher, coupled with the fact that a Controlling Authority may actually request the processing to be entirely and immediately stopped, the implications of non-compliance have significantly increased. Additionally, the processor now has a direct compliance with the GDPR obligations, implicating many companies that felt protected by their role in the transaction.

The data controller and data processor definitions are imperfect in practice, as two companies or entities may collect data at the same time or one collect it for the purposes of its control by another. Imagine buying a phone from a manufacturer and then adding the cellular carrier's service to it. When one or the other party utilizes a cloud provider to host the data or the process by which the data is collected, another complexity enters the model. The GDPR's Article 26 (in a slim 176 words) contemplates the possibility of "Joint Controllers," but the market realities of commercial transactions in our data-intensive business requirements are far more complicated. The Joint Controllers are those situations "[w]here two or more controllers jointly determine the purposes and means of processing,"

but contrast this with where one controller determines on purpose and means and another a second distinct purpose and means, what we have typically called "Co-Controllers." For Joint Controllers, there is no GDPR requirement for a Data Processing Agreement, but rather the requirement is that there be "an arrangement" betweenthe parties. Whether this is a Data Sharing Agreement or something less formal is left to the parties to determine at this point. The Co-Controller is not acknowledged in the GDPR (nor was it in the Directive), but it is a construct that exists extensively in data transfers.

Additionally, with the essentially pan-European scope of the GDPR, and a number of countries with Directive-styled data protection legislation in place, the GDPR becomes the baseline for compliance for international trade and multinational corporations. Much like the Sarbanes-Oxley Act and the Gramm-Leach-Bliley Act, which came into play in the United States with compliance fanfare and have now become laws that transactional lawyers handling covered companies (and/or having covered companies as their customers) are expected to handle with agility and ease, transactional work that includes GDPR and its constructs will likely fall increasingly on non-privacy specialists.

DISTINGUISH THE SECURITY OF THE DATA AND RIGHTS OF A DATA SUBJECT

Every organization is going to have differences in the data it collects, uses (or processes), creates, and needs to protect. There are legal requirements around this data in two separate concepts, however, that must be distinguished – and that may help the organization develop a posture about the risk associated with data generally. The GDPR and many of the country laws that derive from it, have separate requirements around protecting the data and the protection of the rights of the data subject. The protection of the data under the GDPR flows from the rights of the individual and encompasses concepts larger than those we find in the United States' legislation, including a requirement that the data be protected from destruction, unauthorized modification, and that organizations implement Disaster Recovery and Business Continuity Planning programs to protect the sanctity of the end user Data Subject's data and rights. Distinguishing this concept of privacy from the concepts of information security may be helpful in order to organize both transactions and a risk appetite, especially

when customers tend to think that the full InfoSec protections should apply to any data that belongs to them, and not just personal data.[16]

CONSIDERATIONS BEFORE, DURING AND AFTER THE NEGOTIATIONS AND THE CONTRACT

Again, while certainly not all-inclusive, the following list should help in framing a process for handling data-rich transactions. While much of the following advice will practically end up in the Data Processing/Transfer/Protection Agreement ("DPA"), some of it is necessary for the appropriate creation of the DPA and may need to be reflected in the body of the agreement and in the process of performing the contract. Other sources have covered the importance of the DPA,[17] and each entity should create (and evolve) a DPA that reflects its risk posture and its business in accordance with its informed interpretation of the GDPR.

1. Determine who is doing what, where, when, and how – at this point in time

Ideally, data protection and privacy attorneys have had a robust understanding of the deals that they have been asked to opine upon, but in practice questions asked may be targeted and narrow. Under the GDPR, a lack of understanding of the whole of the deal – as well as an understanding of what the deal could become – may be a risky proposition. Consider the following in order to best craft robust protections for your party:

a. Who are the data subjects? Are they employees? Employees' dependents? Customers in a corporate sense? Consumers? Are there children within the universe?

16. See Jeimy Cano, Privacy and Information Security: The Territorial Challenges https://iapp.org/news/a/privacy-and-information-security-the-territorial-challenges1/, especially Figure 1 (last visited March 5, 2019).
17. See Phil Lee's blog entry from October 28, 2016, which stands the test of time, The GDPR will set the benchmark for global privacy contracting – and here's why" available at http://privacylawblog.fieldfisher.com/2016/the-gdpr-will-set-the-benchmark-for-global-privacy-contracting-and-heres-why/ and the UK's Information Commissioner's Office GDPR guidance: Contracts and liabilities between controllers and processors, available at https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf (both last visited March 5, 2019).

b. What data is in play?

   i. Non-special personal data, including Contact information? Computer or device identifying information? Transactional information?

   ii. The GDPR defined "special categories of personal data," which includes "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data [as defined in Article 4(13)], biometric data [as defined in Article 4(14)] for the purpose of uniquely identifying a natural person, data concerning health [as defined in Article 4(15)], or data concerning a natural person's sex life or sexual orientation"?[18]

   iii. Criminal offense data?

   iv. Non-identifying data?

   v. If the transaction involves the special categories of data, ensure compliance with the rest of Article 9.

c. What is happening with the data? Many companies have spent extensive amounts of time mapping data flows within their organizations. Some of these methodologies may be robust enough to take to deals, but to properly orchestrate contractual protections with the other party and that comply with the expectations of the GDPR itself, it is crucial to understand what is being collected, when it is being collected, if that collection is direct from the data subject or if it is occurring without (or possibly without) the awareness of the data subject. Is additional information being collected or added (such as from an additional data feed or match from a service)? Is the data subject's behavior or activities creating new data? Does this data stay within the contracting organizations or are there other parties involved in this?

d. Is there a transfer of the data, if so to what entity and where is that entity located? Is the transfer within jurisdictions deemed to have adequate measures for the protection of the data (as required by Articles 44-49, and as obligations to the Controller under Article 24 and the Processor under Article 28)?

e. Are subprocessors being utilized?

18. GDPR Article 9.1.

2. Determine who *could* be doing what, where, when, and how – contemplate possible scope creep

Given the core business lines in which the parties perform, and focusing most on the other party and what services and/or products it offers, imagine how the transaction or engagement could grow. If the transaction were to grow, especially under a Statement of Work or a Purchase Order, where a new contract might be unnecessary, what data-centered activities could expand?

Where the expansion should involve a new master agreement, determine what controls are in place to ensure that it is also reconsidered. This is a difficult issue for service providers, who may be handling one type of data under a master agreement and an initial statement of work, but should a very different type of data be implicated by a new statement of work, would the right people know about it and be able to modify or renegotiate the main agreement or an associated DPA? Remember that there is the expectation if Model Clauses or Standard Contractual Clauses are used that the data and the data subjects are defined with a level of specificity.

Additionally, consider how the relationship could organically grow to the benefit of both parties. What would need to be revisited? Should the main agreement expire so that it is revisited?

3. Consider the rights of the data subject and the data subject's right to control his/her data

Refocus on the purpose of the GDPR, perhaps by considering Recital 1:

> "The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her."[19]

And Recital 4:

> "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications,

19. GDPR Recital 1.

> the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."[20]

While these may seem lofty aspirations and far from the concrete provisions of a contract, considering the foundational rights of the data subject and the data subject's right to control his/her data helps roots us in the purpose for many of the requirements under the Regulation, and helps where there is uncertainty and imperfect definition, especially in the upcoming considerations.

4. Define the positions of the parties as controller or processor and consider the role of the cloud

Determining which party is playing which role (even if they both play one of the roles at one time in the process) aids in determining how to structure the contract.

a. Is the agreement a business to business or business for business transaction? Business to consumer? Are there cloud dimensions to it? If so, what is the role of the cloud provider?

b. Is there processing that would qualify as automated? If so, consider the Article 29 Working Party's Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.[21]

c. Finally, who is the controller – or which entity is mostly the controller? The processor? What subprocessors are involved, if any?

An additional aspect to many data transactions now is whether the data remains in an on-prem data facility or is processed or stored in the cloud. While on-prem solutions once meant a great deal more control by the entity responsible for the data, now they may be hybrid solutions with cloud processing, storage, or transmission. If the data is hosted or processed in the cloud, knowing the type of cloud (public, private, hybrid, etc.), the provider, and the extent of the data held within the cloud is important. Additionally, even on-prem data may send telemetry to another system (owned by the other party or even a fourth party) and customer service and support teams may be able to access

20. GDPR Recital 4.
21. Available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (last visited March 4, 2018).

data. The extent to which these elements are involved in the deal should be clarified as part of the transaction.

5. Determine the relative responsibilities under the GDPR

The Regulation imposes substantive responsibilities on the parties. Many of the following find themselves in a good DPA, but not all, and are generally the obligations of the processor. Consider the following and how the contractual provisions will capture what should happen:

a. Security. Which party and to what degree at the obligations for security of processing under Article 32 to be met? How is each party "[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"[22] and what are the expectations around anonymization, pseudonymisation, and encryption between the parties?

b. How is lawful transfer handled? What will happen if Privacy Shield is ruled invalid?

c. How is lawfulness of processing being assured?

d. How are audits defined and how are they executed? With what frequency? What is the interplay between offering audit rights and protecting other customers' confidentiality?

e. Who will handle notice in the event of a breach?

f. How will the record-keeping requirements for the processing be handled?'

g. Are the technical and organizational measures and the security expectations between the parties in line with the type and amount of data that will be collected, processed, and stored?

h. Will there be a general or a special authorization to use sub-processors? How is the right to oppose to the designation of a new subprocessor handled?

In considering transfer lawfulness, remember that Privacy Shield only handles E.U. to U.S. (or Switzerland to US, if the Swiss Privacy

22. GDPR Article 32.1.

Shield is adhered to as well) transfers, and Business Corporate Rules ("BCR's") only transfers amongst a given group of companies (namely affiliates). Also remember that other countries may have specific requirements, such as the Argentinian Standard Contractual Clauses.

Be careful with absolute data residency promises. Don't forget about customer service functions that may be following the sun. Payment information that includes customer business contacts and flows back to the U.S also. can contradict residency. Make sure to allow proper carveouts if data is not all kept in the home jurisdiction. Consider also system health data (that may contain IP addresses and other computer identifiers) and any other "phone home" systems.

6. Consider the operational requirements under the GDPR

Consider how to comply with the operational aspects of the GDPR in the contemplated transaction with the contemplated activities. For some entities, this may be a one-time consideration, but if additional promises are made within some agreements – audit provisions or sending updated reports of compliance, for instance, this will need to be operationalized. Other operational considerations include:

a. The obligations around Data Subject Access Requests. Consider which party holds the obligation and what happens when a request is misdirected.

b. Notice of subprocessors. Will the processor notify via SNS or SMS or email or on a website? The GDPR requires a right to object to a specific subprocessor within the notification process, how will this be handled between the parties?[23]

c. Naming a contact for questions from regulators and data subjects.

7. The worst-case scenario game: Imagine what could possibly go wrong

Consider the absolutely worst-case scenario and think through how it happens and what insurances you should be taking. Is it a bad actor or is it a confluence of highly unlikely events that could devastate both parties? What is the likelihood of harm? In information security models, the devastation and the likelihood of the event taking place are

23. In practicality, how the right of one company to object to a new subprocessor of another company remains to be determined.

multiplied to determine the potential size of the event. How would it be survived and what can be done in the contract to assist this?

a. Consider the traditional contractual elements of limitation of liability, insurance, indemnification. Think about the cost of cleaning up the worst-case event. Can you put a number on the cost based on what we know about the super breaches and from the annual reports on breach? What would notification obligations and protection post-incident potentially cost? Who would pay a regulatory fine and how?

b. Consider the standards for liability in the agreement relative to the worst case. Is it appropriate? Is each party accepting appropriate responsibility for its actions?

c. In looking at the limitations of liability, consider if there is a difference in payout at different points in the agreement. Some agreements have "paid to date" clauses, while the cost of a data breach likely would not change based on the payment situation of the parties.

d. Be wary of limitation of liability caps and craft carve outs very carefully. Is a violation of law, negligence, willful misconduct a standard? Limitation of liability for data breach are becoming increasingly complex.

e. Consider indemnification. Is it necessary?

f. How could the harmed party be made whole or the potential harm reduced?

g. How could the data subjects be made whole or the potential harm reduced?

h. Who would contact affected data subjects and control any messaging? Would credit reporting be offered and by whom?

8. Consider the interplay between Data Processing/ Protection Agreements (and/or Data Transfer Agreements) and the main agreement

Ideally this interplay has been foundational to the other considerations, but the agreements need to work together to protect the parties. Is it clear which provision for liability if both have one prevails? Do they intersect properly? If the DPA was an addendum, does it invalidate language (often significantly different) in the main agreement?

Another consideration is that many of our Data Agreements have been focused on the GDPR either explicitly or in their focus. For this reason, the main agreement may be a better place for general contractual terms that the parties would want to apply regardless of where an issue arose.

9. Consider an endgame and cleanup

The processor has an endgame obligation to destroy or return the data to the controller under Article 28:

> "[A]t the choice of the controller, [the processor] deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data."[24]

But for many complex service providers and partnerships, this is much easier described above than put into production. Considering whether the agreement has any specific data needs that should be considered at the endgame in advance of the endgame can make the conclusion much less painful.

10. Reconsider the Deal and the Data Lifecycle – and Monitoring Obligations

Consider the reasons behind the deal – why was this party selected for this relationship, what do they offer better or different than the rest of the marketplace? Review the Fair Information Practice Principles (the 2013 OECD update version:[25] Collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability) and make sure the risks and responsibilities of both parties in regard to these principles have been addressed. Similarly, consider the flow of data and any augmentation that could or will happen as part of the deal.

Reconsider the end game mentioned above. And finally, consider whether the deal invokes the sorts of relationships, whether based on risk factors and data types or whether of the sort of controller and processor or because of the services provided in which an expectation of monitoring and ongoing review of one party by the other (or each

24. GDPR Article 28.3(g).
25. See The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf , p. 75, Box 1 (last visited March 5, 2019).

by the other) should take place. Does this obligation to monitor flow down beyond the party and on to its subprocessors as well (often the case when providing services or goods to regulated industries)? Is that an obligation the party is willing and able to meet? Is there a regulatory obligation or a desire based on risk for audits or annual security questionnaires or some activity in the middle? Do the parties share their understanding of the extent of that activity, both in terms of the time that it will take the entity being reviewed and the intrusiveness of the questions? Especially with multinationals and companies in regulated industries, ensuring that there are no surprises with the obligations for transparency regarding information security practices and policies will make for a better long-term outcome between the parties.

CONCLUSION

The past year has seen the GDPR change many things, and for those of us working with data transactions, there are new concepts and requirements that need to be integrated into our practices, templates, language, and processes. The emphasis on making sure that parties acknowledge risks and divide the responsibilities for protecting data between themselves requires both sides of the transaction to understand the deal and its associated data more deeply. The questions above change in both relevance and in response as the deal changes scope, risk discussions evolve, and the opportunities for future work between the parties grow. Hopefully, with time will come additional clarity in the form of additional pragmatic guidance from the regulators about their expectations.

NOTES

30

Managing Vendor Risks in a Changing Regulatory Landscape (March 11, 2019)

Maureen A. Young

Bank of the West

The views expressed are Maureen Young's alone, and not those of Bank of the West.

[Article, including Appendices A, B and C]

At past sessions of the PLI Institute on Privacy and Data Security Law, we have discussed key practice tips for the successful oversight of third party service providers. We have talked about approaching third party risk management as a life cycle that begins with developing a strategy for use of third party service providers, where potential relationships are thoroughly assessed and the key terms for the service relationships, including appropriate privacy and data security standards, are well-documented and supported by performance monitoring on a continuing basis, and through establishing terms and processes for eventually exiting the relationship, with recovery or verifiable destruction of confidential data. To refresh ourselves, some fundamental vendor management practice tips ("oldies but goodies") are summarized below, with a full outline of these practice tips set forth in Appendix A at the end of these materials. Please also review the additional practice tips discussed at recent PLI meetings in Appendices B and C.

1. Approach third party service provider risk management as a life cycle.
2. Develop your strategy for use of third party service providers.
3. Take a broad view toward the scope of due diligence required. Identify and assess all potential risks and give special focus to the highest risk areas.
4. Identify the service providers that perform the most critical activities for your company and conduct enhanced due diligence on them and seek additional controls for those relationships.
5. Plan for achieving leverage in the selection of and negotiation with vendors.
6. Develop template vendor agreements and seek key contractual protections.
7. Pay special attention to the unique privacy and security risks of a service arrangement.
8. Plan for service interruption and service performance issues.
9. Conduct ongoing monitoring of the vendor, particularly for your critical relationships.
10. Plan for termination scenarios. At termination, verify to ensure all sensitive information is returned or destroyed.

This year, we are once again taking a deep dive into third party service relationships, focusing specifically on building vendor management programs to comply with privacy and cybersecurity requirements, particularly in light of recent legal and regulatory developments.

Over the past year, the focus on privacy and data security protection has continued its upward spiral, resulting in more data and security laws, regulations and guidance being enacted in the U.S. and around the world, adopted in response to yet more major security breach incidents, as well as the exposure of insufficient corporate controls to prevent significant data misuse, and heightened concern for privacy rights in the response to deployment of new technologies, using facial recognition and other biometric data and geolocation data.

The past year also saw the enforcement date of the GDPR, the effective dates of most requirements under the New York State Cybersecurity Regulations, and the passage of the California Consumer Privacy Act (CCPA), which is heavily discussed addressed in this year's PLI program. The California law also triggered other states, such as New York and Washington, to consider legislation along similar lines.

Other new laws affecting varied privacy and security areas were enacted in California (Internet of Things and also bots/artificial intelligence), Colorado ("reasonable" security standards), New Jersey (limiting a merchant's ability to pass consumer data on to third parties), Ohio (cybersecurity safe harbor bill), and Vermont (data brokers).

New state security breach notification laws were enacted in Alabama and South Dakota, and expanded state security breach notification laws were adopted in Arizona, Colorado, Louisiana, Massachusetts and Oregon.

The passage of the CCPA, together with the Equifax, Marriott and other breaches, has stirred again the potential for federal legislation. But while many different federal bills have been discussed or proposed, the likelihood of Congressional agreement in the next two years on any one omnibus scheme seems doubtful.

The past year also brought a refresh of the NIST Cybersecurity Framework (core functions to identify/protect/detect/respond/recover), which included an expanded section on cyber supply chain risk management. In addition, work commenced toward a draft NIST Privacy Framework (core functions to identify/protect/control/inform/respond).

At the same time, around the globe in India, China and elsewhere, more nations have adopted new statutory privacy and security requirements.

All of these regulatory developments help inform us of areas to emphasize, update or revise in our vendor management programs for the

coming year. We turn then to our 2019 top ten tips for vendor management compliance.

2019 TOP TEN TIPS FOR ENSURING COMPLIANCE WITH PRIVACY AND SECURITY REQUIREMENTS IN THIRD PARTY SERVICE RELATIONSHIPS

1. **Expect and plan for a continuing patchwork of varying and often conflicting state laws, regulatory standards and industry framework guidelines that will impact the privacy and data security controls your company needs to impose on your vendors, in addition to your company's own controls.**

   In the U.S., there is no sign that on a federal level an omnibus comprehensive privacy and data security framework standard will be adopted any day soon. We will continue to operate under a complex legal and regulatory framework. That is particularly true for companies with global operations that must also comply with varying country standards. It is often said that the implication of such a legal patchwork is that a company must "comply up" with the most restrictive standards, which is good advice, but it is also the case that your company may need to comply with very specific and different requirements to meet the varied state and country standards. In light of this complex and changing environment, your company may wish to:

   - Formalize a "regulatory watch" function within your company to track new legislative and regulatory requirements impacting your domestic and global business operations and assign responsibility for assessing and implementing the changes to specific business functions, and identify which of these changes will require revisions to your third party service arrangements.
   - Review the contractual provisions in your outsourcing agreements to determine if they permit you to amend the contract specifically to conform with new privacy and security standards in the face of regulatory and industry change.
   - If material changes need to be made, you will likely need a contract mechanism for resolving how the costs related to required or requested changes will be borne between the parties, and an exit ramp for your company if the parties cannot agree on the costs, the implementation timeframe, and/or the value of continuing the outsourcing arrangement under changed circumstances. With this, you also will need to have identified in

advance acceptable alternative service providers as your contingency plan.

- Plan for a longer timeframe for the periodic contractual review and renewal process. With many changes to laws and industry standards, your company's model vendor agreements will require more revisions, and consequently, negotiating amendments in your vendor contracts will also require a longer ramp time.
- Assess from the outset if you need to choose a vendor that commits in writing to providing a product/service fully compliant with all laws and regulations applicable to your company as the service recipient, particularly if your vendor is non-U.S. entity. "Compliance with laws" provisions in service agreements often state that the parties will comply with "all applicable laws," meaning all laws applicable to each of them respectively. Service agreements may also provide that the service provider will comply with laws specifically called out in the contract as applicable to the service recipient. But if your company will have difficulty tracking regulatory changes or negotiating changes with the vendor after the agreement is executed, you may wish to choose a vendor offering a "globally compliant" product.
- In the due diligence process, gain a good understanding of what legal and regulatory framework directly covers your vendor's operations so you may focus on areas where there may be gaps between the framework to which your company is subject and to which the vendor is subject.

2. **In light of more expansive definitions of personal information under recent laws and regulations, review the definition of personal information under your company's data classification policy and update accordingly. Revision to your company's data classification regime is likely to also require revisions in your vendor contracts on how personal information is defined and treated.**

    - Recent laws have added more data categories to the definition of personal information. This is a trend continuing in pending legislation, but your company's data classification policy may not be up to date. For example, the sharing of employee contact information may not be treated as confidential information in your vendor contracts, but depending how the CCPA may ultimately be amended or interpreted, such data may constitute

personal information for which the subject employee may exercise statutory rights. Similarly, biometric or geolocation data may not be included in your defined elements of protected personal information, which should now be defined very expansively consistent with the CCPA, GDPR and other laws.

- Establish formal employee data privacy and security policies and procedures. U.S. companies, particularly those without European operations, may not have formally established employee data privacy and security policies and procedures because of the absence in the U.S. of a federal employee data privacy and security "sectoral" law akin to the frameworks required to protect financial, health, educational and children's information. Companies have historically considered whether certain corporate practices align with employees' "reasonable expectations of privacy" as defined under case law and have included disclosures and disclaimers on workplace expectations of privacy in employee handbooks, and have also adopted required policies protecting employee personal health information under HIPAA. But given the inclusion of employment-related information in the CCPA, GDPR and other laws, companies should be assessing and formalizing their employee data privacy and security frameworks. This will have impact as well on what requirements you impose on vendors handling your employee data.

3. **Focus on a better mapping of data housed in different systems and ways to effectively access or interconnect those systems for data searches and retrieval. Gain an understanding of how your vendors store your company's data and their ability to search for, retrieve and delete it.**

    - Many companies have grown over time and through various transactions, acquiring a multitude of systems for different purposes with separate databases. The implementation of the CCPA and other laws will require companies to do an assessment and mapping of these data-rich systems to see where personal information (as now broadly defined under recent laws) is stored and how it can be retrieved and deleted.

    - Data mapping against system inventories will be necessary to support individual privacy rights protected under the CCPA and other laws, enabling a company to provide advance notice about what personal information has been collected about them and

respond to a consumer's request for a tailored letter addressing the categories and specific pieces of information collected, and/or respond to the consumer's request to delete that data.

- Companies will need to develop contractual terms to amend existing and include in new contracts that impose requirements on service providers to cooperate with the company's obligations to provide tailored responses to consumers and effectuate data searches and their deletion requests.
- It will not be enough to just obtain contractual commitments from your vendor. You will need to add to your due diligence review an assessment of the vendor's network of systems holding your data and the vendor's ability to effectuate deletion requests.
- Because many companies' systems are not interconnected, it may be years before companies are able to create automated ways to search and delete data across all systems. Manual retrieval and deletions may be required for near term compliance.

4. **More laws adopting broader definitions of personal information, enhanced consumer privacy rights, and heightened security standards and security breach liability obligations means companies will need to further enhance their due diligence conducted on service providers.**

   - Few privacy and security laws actually dictate what the scope of or what specific due diligence elements have to be reviewed about a vendor.[2] Instead they posture that if a company decides to outsource activities to a vendor and share protected data with that vendor, the company remains fully responsible for the privacy and security of that data. Some laws, such as the NYS Cybersecurity Regulations, require that the company maintain a third party service provider security policy, which must address such elements as identification and risk assessment of the third party service providers; minimum cybersecurity

2. An exception here is the regulatory regime for financial institutions. Financial institutions are subject to specific regulatory guidance as to the scope of due diligence that must be conducted and the elements that must be reviewed for a third party service provider. See the resource materials listed at the end of Appendix A.

practices required of such service providers; due diligence processes used to evaluate the practices of the service provider; periodic assessment of the cybersecurity practices of the service provider based on their risk, etc. Specific legal requirement or not, having a well-developed and documented vendor due diligence and risk management program is critical to meeting privacy and data security obligations.

- As we have discussed in other years, it is important that the company have assessed each service provider's Inherent Risk Profile and have risk ranked its various service providers by criticality of the activities performed and sensitivity of the data shared with them. Service providers with the highest risk ratings should be subject to enhanced due diligence, more developed contractual controls and more extensive monitoring.
- Your company should conduct due diligence based on assessed risk levels, including reviews of, for example:
    - Financial and credit risk;
    - Performance risk;
    - Strategic risk;
    - Legal, regulatory and compliance risks;
    - Business reputation risk;
    - Operational risk;
    - Transaction risk; and
    - Special risks (e.g., sensitivity and scope of the data shared; offshoring arrangements presenting more challenging supervision risks, country risks and other risks; multiple layers of subcontractors; complexity of the service relationship; cross border data transfers; information stored in cloud).
- Because adequate due diligence is so important in selecting a competent vendor and enhanced due diligence on critical vendors requires an extensive review and assessment of data, many companies are seeking more efficient ways to conduct due diligence. Efficiencies are developing through:
    - The establishment of commercial third party due diligence repository systems, which allow companies to acquire

common due diligence portfolios on certain vendors. Although the diligence captured in these databases may be baseline, requiring your company to conduct additional diligence tailored to the risks of the specific service relationship, the databases offer an expedient way to acquire information, which also is updated regularly to support periodic reviews.

  - Global companies with multiple subsidiary operations are seeking consents from vendors to confidentially share due diligence information within the company to support efficient vendor assessments.
  - More companies are using automated vendor questionnaire and assessment tools to capture and compare vendor assessments, and to support the efficient delivery process for requesting updated vendor assessment information.

- It is important that your company's vendor questionnaires be updated periodically to capture changes in privacy and security laws and learnings from recent security breaches. For example, in response to the CCPA, your questionnaires should now assess a vendor's ability to delete individual consumer data records upon request during the engagement, and not just the ability to return or destroy data at the end of the engagement.
- Vendor questionnaires should also be tailored to address the risk of specific vendor relationships. For example, companies using cloud services often have reduced visibility into and controls over the operations of their cloud providers. Cloud service arrangements require enhanced due diligence so that the risks surrounding the nature of the particular cloud service and deployment model are well-understood and assessed and so that there is a clear understanding of what data security obligations are assumed by the company versus the cloud provider. Multi-tenancy cloud arrangements increase the chance of data compromise if the separation controls among multiple tenants fail. It may be more difficult to verify in a cloud arrangement that a company's data has been completely and securely deleted.

5. **Vendor due diligence should evaluate all aspects of supply chain risk, including the culture, ethics and compliance practices of service providers.**

   - In the aftermath of the Cambridge Analytica and other incidents at social media and internet companies, more focus is being placed on evaluating a company's "culture of compliance" and its "supply chain ethics" in passing through to its vendors comparable standards of transparency and fairness in how customer data is used, protected from further disclosure and secured. Through the due diligence process, companies can obtain information to make informed decisions on selecting vendors that "fit" with the company's culture and practices.
   - Support for supply chain ethics includes choosing vendors that have adopted a Code of Conduct and related policies and procedures that align with the culture, ethics (including data ethics) and compliance practices embraced by your company. The Code of Conduct should be supported by training of staff and special training at the executive level.
   - Companies may wish their vendors to also align with the PIC (Protecting the Interests of Customers) program adopted by your company in an effort to put consideration of the customers' interests, including their privacy rights, at the forefront of business decision-making.
   - Many European and other companies have adopted detailed Corporate Social Responsibility (CSR) programs[3], where, here too, it would seem important to use the due diligence process to support the selection of vendors that align with the company's CSR objectives.

6. **Contractual controls over service providers are only as protective as the company's ongoing monitoring activities supporting them.**

   - Many companies have already developed template vendor contracts with a good plate of contractual protections, such as requirements that the service provider develop and submit for

3. See the European Commission's Guidelines on Corporate Social Responsibility, https://ec.europa.eu/growth/industry/corporate-social-responsibility_en.

the company's review and approval a written information security plan and a business continuity plan; submit at least annually financial reports and operational and SSAE 18 and other security-related audit reports; and required standards for employee and subcontractor personnel. But if these reports are not reviewed and assessed by the company or monitored for compliance, the contractual clauses fall short of their purpose.

- In years past, the primary responsibility for the vendor contractual relationship at many companies often lay with the business line, which may not have had time or focus to support ongoing monitoring of vendor risk issues, particularly where emerging problems are not readily apparent. To achieve better ongoing assessment and monitoring of the vendor's condition, many companies have established vendor risk management teams units that are expressly dedicated to ongoing vendor monitoring and assessment activities. Vendor monitoring can be supported by system records documenting key contractual requirements. Tracking of the areas where the vendor needs to provide regular reports is key, and so is having these reports reviewed by staff with sufficient subject matter expertise to identify areas of potential concern.
- Don't let your company rely on "pat" contractual clauses, the vendor's compliance to which is not investigated or enforced. For example, many companies have terms requiring that a vendor's and its subcontractor's personnel undergo background checks meeting specific search requirements.[4] But once the contract is signed, is your company seeking confirmation that the background checks are being conducted and completed in accordance with the required scope before the vendor's personnel are on-boarded and given access to your company's data? And are the background checks being updated regularly? Although there has been much media attention focused on on cybersecurity attacks by external threats, it is still the case that many breaches come from the "threat within."

4. Financial institutions, for example, are required to have vendor personnel background checks be conducted consistent with Section 19 of the Federal Deposit Insurance Act, which puts no time limit on the lookback for criminal convictions.

7. **Review and improve "fourth party" due diligence, contractual terms, and monitoring.**

   - For some time, companies relied on contractual commitments with a service provider that the service provider would take full responsibility for the actions of any subcontractor and would require its subcontractor to agree in writing to privacy and security and other terms and conditions at least stringent as those imposed on the service provider itself. Companies also took comfort in including contractual terms requiring the company's prior consent before a service provider could subcontract its work out to another party. Although these are still important contractual protections to include in your vendor agreements, with continuing data security incidents occurring at vendors, it is important to look closer at fourth party relationships.
   - Before consenting to a service provider's use of a subcontractor, the company needs sufficient information about the subcontractor and adequate contractual rights. Where the fourth party will have access to personal data, the company should conduct due diligence, including a security assessment on the fourth party, to the extent appropriate depending on the risks of the arrangement. Although the service provider can assist here by providing information and coordinating with its fourth party, it is important that the company have sufficient information to make an independent assessment of fourth party risks.
   - Contractual clauses should also include requirements on the service provider to conduct audits and security reviews of its subcontractor to the company's satisfaction, and also provide the company with the option of the conducting the audits and security reviews itself on the fourth party.
   - The contract should provide that the fourth party must accommodate access for reviews by the company's regulators and external auditors.

8. **A company's vendor management program should address the specific risks related to using offshore service providers.**

   - As companies look for the efficiencies achieved by services being performed in lower cost jurisdictions, as well as by incorporating new technologies and special expertise, the globe gets smaller and smaller. But reliance on foreign-based third

party service providers raises special country, reputational, operational/transactional, compliance and strategic risks that need to be assessed, reviewed in the due diligence process, and addressed through protective contractual provisions and through the company's vendor monitoring and oversight procedures.[5]

- The company should assess the country risk associated with the foreign service provider, including conducting an analysis of the economic, social and political conditions in the foreign country that may adversely affect the ability of the service provider to perform and which, depending on the circumstances, may lead to a rapid decline in the service delivery. Due diligence should also include an evaluation of the potential impact of the foreign jurisdiction's laws and legal environment, regulatory requirements, local business practices, and tax and accounting standards. Background checks of personnel are not easy to get completed in some countries because of inadequate records and/or legal restrictions.
- As you are well aware, countries have different privacy and data protection regimes, which in some instances restrict the ability of a U.S. company promptly obtaining information once offshore about individuals in response to litigation demands or regulatory requests. For these and other business continuity reasons, companies should consider requiring full back-up copies stored in the U.S. of data processed offshore.
- The offshore jurisdiction presents challenges for the ongoing monitoring and supervision of the service provider, particularly in the instance of fourth party service providers. Time difference, distance, and culture should all be evaluated in determining whether the company will be able to regularly engage to supervise and effectively monitor the service provider's activities.
- Different corporate and structural alternatives may facilitate a company pursuing offshore service activities, such as the formation of the company's own offshore captive subsidiary. But other control mechanisms that still directly rely on the third party

5. See, for example, Federal Deposit Insurance Corporation, 2006, Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers https://www.fdic.gov/news/news/financial/2006/fil-52-2006a.pdf.

service provider model are available. In the case where the offshore service provider is in a high risk country and is processing personal data of the company, the company may wish to require that the service provider provide the services through an Offshore Delivery Center (ODC). The ODC is designed to establish a highly secure segregated workspace where designated workers' activities are monitored through access controls.

- Contractual terms specifying that the service provider perform the services within the confines of an ODC might include controls such as the following:
    - Dedicated teams who work only on services for the company; knowledge wall separating these workers from other workers of the service provider supporting other clients;
    - Physical structures (building and floors) that are vendor-controlled;
    - All work performed in the secure workspace with physical security controls such as logged secured access, camera coverage, and inspection of personal items on entering and existing the workspace;
    - All endpoint devices housed within the secure workspace, including: network connectivity (meeting the company's standards, including standards for redundancy and resiliency); thin client/zero client devices; hard tokens (including token storage lockers); keyboards; mouses and monitors;
    - Equipment dedicated to the performance of the company's services must be physically located in the secure workspace and logically isolated (permitted to communicate with only specifically identified vendor support resources);
    - Heightened incident reporting;
    - Prior authorization and escorts for visitors; and
    - Prompt notice to the company when users are terminated or missing any multifactor access token.

9. **Customer data is better protected when the contract contains clear, multi-level metrics for service provider performance standards; a cadence is established for the vendor's submission of specific reports on these metrics; regular meetings for reviewing service provider performance metrics are required; and when an escalation process is documented for circumstances where ongoing performance problems arise.**

    - Too often the business is anxious to get the contract executed so the services can commence, but has not spent sufficient time in developing performance metrics to evaluate the services. The vendor risk management team needs to push back on the business to ensure that adequate performance evaluation standards are developed before the contract is executed and monitored during the engagement.
    - Consider investing in automated tools for tracking vendor performance against contractual standards and vendor reporting.
    - Data security protection requires well-developed obligations for the service provider to maintain systems and processes to test, detect, log and report unauthorized access attempts and promptly report security incidents to the company. While many security incidents do not amount to a security breach requiring legal notice, the vendor should be required to report on its remediation activity for mitigating all security incidents. After a security breach has occurred, the company should conduct a security audit to ensure that the vendor's remediation activities have been effective.

10. **Review and update your vendor risk assessment process, contractual protections and monitoring activities to incorporate privacy and data security concerns posed by deployment of new technologies and processes.**

    - In the age of bots and the Internet of Things, many new technologies are being incorporated into a service provider's operations. Your company may have selected the vendor precisely because of the efficiencies produced by the vendor's deployment of new technologies. But these technologies require assessment and implementation of appropriate controls.
    - Artificial intelligence (AI) and machine learning are being used at an increasing rate to realize improved processing times. It

is important that your company knows how and where AI is used, and deploys it in a fair and transparent manner. In 2018,[6] California adopted legislation prohibiting users of bots to communicate or interact online with another person in California with an intent to mislead the other person about the bot's artificial identity to incentivize sales (or influence votes). The company deploying the bot must disclose in a clear and conspicuous manner the bot's artificial identity.

- Regulators are supporting the use of AI to more efficiently collect and analyze data where manual processes are not effective, such as to meet Bank Secrecy Act/Anti-Money Laundering "Know Your Customer" and enhanced due diligence requirements. At the same time, however, they are warning that companies need to have a strong grasp on how AI is functioning and adequate monitoring and testing procedures to ensure that customer data is being analyzed and processed accurately.

In summary, companies cannot let their vendor management programs get "dusty." It is critical to keep up with the changing privacy and security laws and evolving cybersecurity challenges and incorporate changes into one's vendor management program to address the specific legal and regulatory concerns and new threats to consumers' privacy rights and data security.

6. California Senate Bill No. 1001, adopted September 28, 2018.

APPENDIX A

Ten Foundational Tips for Successful Oversight of Third Party Service Providers (excerpt from 2016 presentation)

1. **Approach third party service provider risk management as a life cycle:**
    - Develop a strong third party risk management program that outlines the company's strategy, identifies the inherent risks of the outsourced activity, and details how the company selects, assesses, and oversees the third party.
    - Framework of program should include key governance elements:
        - Three lines of defense (first line is typically business line; second line is risk management teams, e.g., compliance, legal, information security risk management, etc.; third line is audit function)
        - Written policies and procedures
        - Policy and exception variance process and escalation review process
        - Designated responsible internal officers, with delineated roles and responsibilities, e.g., Chief Third-Party Risk Management Officer and supporting team
        - Review and update of the program at least annually
        - Training of key personnel
        - Independent review; periodic audit of program
        - Oversight by appropriate company board and executive management committees
    - Appropriate due diligence in selecting the third party.
    - Written contracts that outline the rights and responsibilities of all parties, containing key protective terms for the company; no undocumented side bar arrangements.
    - Ongoing monitoring of the third party's activities and performance.
    - Contingency plans for terminating the relationship in the least disruptive manner.

- Clear roles and responsibilities of designated officer for overseeing and managing the relationship and risk management process.
- Documentation and reporting that facilitates oversight, accountability, monitoring and risk management.
- Independent reviews that allow management to determine that the company's process aligns with its strategy and effectively manages risk.

2. **Develop your strategy for use of third party service providers.**
   - Assess the risks and benefits of outsourcing.
   - What are your alternatives for vendor relationships versus internal provision?
   - Under what conditions would you enter into a service relationship with a third party provider? What circumstances would be deal-killers for your company? How much complexity in the relationship does your company have an appetite for?

3. **Take a broad view toward the scope of due diligence required. Identify and assess all potential risks and give special focus to the highest risk areas.**
   - The pricing offered is only one consideration in selecting a vendor. Conduct due diligence on all risk levels appropriate, e.g.:
     - Financial and credit risk;
     - Performance risk;
     - Strategic risk;
     - Legal, regulatory and compliance risks;
     - Business reputation risk;
     - Operational risk;
     - Transaction risk; and
     - Special risks (e.g., offshoring arrangements presenting more challenging supervision risks, country risks and other risks; multiple layers of subcontractors; complexity of the service relationship; cross border data transfers; information stored in cloud).

- All available information should be obtained from the vendor, as well as solicitation of direct responses to particular risk issues. A minimum diligence review might include review or assessment of:
    - Audited financial statements, annual reports, other financial indicators
    - Materiality of the proposed service contract on the third party's financial condition
    - Business reputation of the third party
    - Third party's experience and ability in providing the services; qualifications of the company's senior management
    - Reliance on subcontractors (in and outside of the U.S.); use of cloud providers; reliance on key suppliers
    - Significant complaints, litigation and regulatory actions against the third party
    - Systems capabilities; management information systems
    - Internal controls, including privacy and data security controls
    - Audit reports re: the effectiveness of internal controls
    - Third party's service philosophy, culture and code of ethics for employees
    - Proven knowledge of relevant laws and regulations applicable to the services, such as applicable consumer protection laws
    - Adequacy of business continuity plans
    - Adequacy of insurance coverage
- Line up an appropriate internal team of Subject Matter Experts (SMEs) to conduct the diligence and/or serve as a resource for the company's third party risk management team.
- Have a clear understanding of the service relationships. What subcontractors and suppliers support your lead service providers? Need to conduct due diligence on all these "links" in the chain. Allow no weak links. Are there some relationships for which subcontracting will not be permitted?

- Diligence results should be documented, with supporting risk assessments for each area. Overall risk assessment needs to align with the company's reward/benefits analysis for retaining the third party and its overall strategy for outsourcing functions.

4. **Identify the service providers that perform the most critical activities for your company and conduct enhanced due diligence on them and seek additional controls for those relationships.**

    - Framework should be programmatic and risk-based. Scope and depth of the due diligence conducted should be directly related to the importance and magnitude of the company's relationship with the third party. Rank the vendor relationships by most critical, medium risk and low risk (or some variations of same). Diligence for the most critical vendors should be intense, with more frequent ongoing reviews, and more detailed contractual protections.
    - Assessment of a "critical" third party relationship will focus on different factors depending on the services outsourced, but may include assessment of:
        - What sensitive information is being disclosed
        - Impact of loss on customer confidence
        - Disruption of the company's material operations
        - Significant financial loss through disruption of material revenue streams
        - Potential to incur significant expenses in transferring the relationship to another service provider
        - Potential for significant regulatory actions

5. **Plan for achieving leverage in selection of and negotiation with vendors.**

    - Too often the business moves ahead with its decision on a vendor based on price and ability of the vendor to perform the services on the timeline desired, impairing the company's ability to create leverage in the selection of and negotiation of terms with the vendor.
    - Need to get the business teams to align with the internal third party risk management process to ensure that the company

selects a vendor meeting risk management concerns and which commits to key vendor risk management contractual provisions.

- Although admittedly "size matters" in exercising leverage on a vendor, even smaller companies can take measures to create leverage.
- RFP process; binding responses in writing; early commitment to key contractual provisions or disclosure by the third party of requested variances from the key provisions; running side-by-side discussions with potential service providers; holding out carrots for potential other work.

6. **Develop template vendor agreements and seek key contractual protections.**

   - Develop your own template agreements; lead with your template, present it first; and require commitment by the vendor to template contractual provisions or disclosure of requested variances from these provisions in the RFP process.
   - Seek key contractual provisions that tie into risk concerns:
     - Performance/service level commitments
     - Confidentiality provisions and express privacy commitments as applicable to the services
     - Information security plan and specific security requirements
     - Information security breach notification; duties to cooperate and promptly remediate; provisions to cover costs related to the breach, including credit monitoring service as appropriate
     - Business continuity plan; tie in with force majeure clause
     - Broad compliance with all laws, regulations, with call-outs for specific compliance issues;
     - Specific commitments to company policies and procedures as appropriate
     - Representations and warranties
     - Indemnifications

- Carefully negotiated limitations of liabilities (including no liability caps for breach of confidentiality and security requirements)
- Subcontracting provisions (Permitted? Permitted with prior consent? Offshore subcontractors permitted?). Key contractual commitments also need to apply to subcontractors.
- Service provider commitments for its personnel (employees and representatives); background screening; grounds for removal
- Insurance coverage
- Provision at least annually of financial reports; financial responsibility terms
- Provision at least annually of operational and SSAE 18 and other security-related audit reports
- Company's right to inspect and audit third party service provider
- Assignment clause (permitted with consent or not?)
- Termination rights
- Transition support rights
- Return/destroy at termination of company/client information

- Requires experienced and strong sourcing and contracts team. Do you have the right team? How well do they work with Compliance, Legal and other stakeholders? Quality of their training programs.
- Contractual negotiations require sourcing and contracts team to reach out to internal Subject Matter Experts on specific proposed contractual revisions.

7. **Pay special attention to the privacy and security risks.**
   - Review/mapping of data flows from your company to service provider and its subcontractors; what data being shared and how transmitted, under what security protections; what data flows back to your company from service provider and its subcontractors.

- Controls committed through specific contractual terms should be commensurate with data risks.
- Special attention to cross border data transfers.
- Special attention to cloud use.
- Special attention to offshore vendors.
- Special attention to subcontractors.
- Internal information security dedicated teams should conduct the review and assessment of the third party's information security controls through surveys, testing and onsite visits as appropriate; include supporting contractual terms.
- How well-developed is the third party's written information security plan? Poor documentation of internal controls is often a tell-tale sign of information security weaknesses. The third party's information security plan should be reviewed, updated and shared with the company for its review at least annually.

8. **Plan for service interruption and service performance issues.**
   - Contractual service level commitments, tied to key service parameters.
   - Ongoing performance reports, including reports re: customer complaints and any access control issues and data leakages.
   - Process for response escalation and remediation; escalating service credits for performance deficiencies and termination rights for material failures to meet service level commitments.
   - Do not allow unwritten informal side agreements or contractual variances to develop; happens frequently in the service level area.
   - Have internal business continuity dedicated teams review and assess the viability and effectiveness of the third party's business continuity plan in light of the specific services.
   - Participate in business continuity tests as appropriate.
   - Assess the consequences to your company of a failure of the third party's business continuity plan.

- In some instances, the negotiation of "step in" rights may be necessary.
- The third party's business continuity plan should be reviewed and updated at least annually and submitted to the company for its review.

9. **Conduct ongoing monitoring of the vendor, particularly for your critical relationships.**
   - Too often solid contractual protections get included in the service agreement, but thereafter, the company drops the ball on conducting ongoing monitoring of the third party service provider. View these ongoing reviews as critical part of your company's third party risk management process.
   - Designate teams and individuals with clear roles and responsibilities for ongoing monitoring of third party relationships.
   - Keep records of the ongoing reviews.
   - Use the reviews as part of the basis for renewing, amending and extending the service agreement.
10. **Plan for termination scenarios. At termination, verify to ensure all sensitive information is returned or destroyed.**
   - Think through and develop strategies for potential termination scenarios. What is your exit strategy? How readily can you transfer the relationship to a new service provider or take it back in-house? At what cost and/or business interruption?
   - The harder it is to transfer the relationship, the more important it is to have conducted enhanced due diligence of the third party provider at the outset, obtained comprehensive protective contractual terms, obtained ongoing reporting, and conducted ongoing monitoring of the provider.
   - Seek appropriate transition support terms.
   - Effective vendor business continuity plans help mitigate the need to terminate the arrangement.
   - How will your company's and customers' information be returned at the termination of the agreement?

- If it is not feasible to have the information returned, what measures, with supporting contractual commitments, can you take to verify that the information has been destroyed or erased from the third party's systems? Where it cannot be destroyed or erased, obtain commitments that its confidentiality will be maintained in perpetuity.
- Consider scenarios in which the termination of the agreement will be contentious and protect through contractual provisions against having your information held hostage.

Helpful Resources:

The resources identified below are financial services regulatory guidance, but are helpful in other industry sectors as well for construction of an effective third party risk management program:

Office of the Comptroller of the Currency, Bulletin 2013-29, Risk Management Guidance for Third Party Relationships
http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Office of the Comptroller of the Currency, Bulletin 2017-21, Third-Party Relationships Risk Management Guidance Frequently Asked Questions to Supplement OCC Bulletin 2013-29
http://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-21.html

Federal Deposit Insurance Corporation, 2008, Guidance for Managing Third-Party Risk
https://www.fdic.gov/news/news/financial/2008/fil08044a.pdf

Federal Deposit Insurance Corporation, 2006, Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers
https://www.fdic.gov/news/news/financial/2006/fil-52-2006a.pdf

Federal Reserve Board, SR 13-19, December 2013, Guidance on Managing Outsourcing Risk
http://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm

Consumer Financial Protection Bureau Bulletin 2012-03, Service Providers
http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf

Federal Financial Institutions Examination Council (FFIEC), IT Examination Handbooks:

Supervision of Technology Service Providers, October 2012
http://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers-(tsp).aspx

Outsourcing Technology Services, June 2004
http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

Information Security, September 2016,
http://ithandbook.ffiec.gov/media/216407/informationsecurity2016booklet.pdf

Business Continuity Planning, February 2015
http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

APPENDIX B

Top Tips for Controlling Privacy and Security Risks in Third Party Service Arrangements (Excerpt from 2017 Presentation)

KEY OVERALL SECURITY TIP:

Incorporate into your company's program for its third party service providers as a best practice (or as a requirement if your company is a covered entity) the information security and cybersecurity controls recently identified by state and federal regulators as reasonable or baseline security standards.

1. **Plan for and contract for change.**

   In just the past year alone, there have been significant legal and regulatory developments in the information security and cybersecurity area, most of which directly address regulatory expectations for third party service arrangements. Some of these regulatory developments are outlined above, but they are by no means an all-inclusive list. The point is that you should plan and contract for continual change. You should assume that there will be more varied and conflicting cybersecurity standards released in the years ahead.

   - Make sure the contractual provisions in your outsourcing agreements permit you to amend the contract specifically to conform with new security standards in the face of regulatory and industry change.
   - You will need provisions requiring an annual security review and assessment of the service provider's security plan.
   - If material changes need to be made, you will also need a contract mechanism for resolving how the costs related to required or requested changes will be borne between the parties, and an exit ramp for your company if the parties cannot agree on the costs, the implementation timeframe, and/or the value of continuing the outsources arrangement under changed circumstances.
   - And, then you will need to have identified in advance acceptable alternative service providers as your contingency plan.

2. **Go for at least minimum achievable security standards for your lower risk service providers.**

   Not all of your company's service providers will be high risk ones performing the most critical services for your company and/or handling the most sensitive information. As we discussed last year, a

key part of developing an effective third party risk management program is conducting a risk assessment with a risk ranking for your third party service arrangements, so resources can be directed at placing special review and controls on the highest risk vendors. For others that are not your highest risk vendors, establish that the service provider's program supports at least minimum achievable security standards. Consistent with the "Pareto 80/20 Principle" embraced by the CIS Critical Security Controls and supported by the California Attorney General's Office, if your service provider can evidence to you that it has adopted at least basic cybersecurity hygiene, such as through implementation of the first 5 CIS Critical Security Controls, that may go a long way in giving you comfort in the due diligence process and an ability to proceed with the negotiations.

The first five Controls again are:

CSC 1: Inventory of Authorized and Unauthorized Devices

CSC 2: Create and Maintain an Inventory of Authorized and Unauthorized Software

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

CSC 4: Continuous Vulnerability Assessment and Remediation

CSC 5: Controlled Use of Administrative Privileges.

One may look at this list and say, duh, this is common sense. But if your service provider is doing it well – has effectively conducted its inventories, is securing configurations on equipment, is continuously assessing vulnerabilities and remediating, and maintains well-developed controls over the use of administrative privileges, etc. – it arguably has reasonable security standards.

- You can go further than just a diligence review documenting evidence of implementation by the service provider of the basic controls by requiring as part of the written contractual terms that the controls be adopted by the service provider and requiring periodic evidence that the controls are still in place and working effectively.
- Support the controls with reporting. In the contract's schedules, have the service provider identify for you an inventory of all systems devices running or storing your data, provide regular reports on vulnerability threats to your data and what remediations were undertaken, and require updated lists of current

personnel with administrative privileges to the systems and devices running or storing your data.

- Administrative privileges tend to get outdated regularly as workforce members move to other assignments. Request periodic reports of focused audits on the use of administrative privileged functions.
- It may be hard for your company, depending on its size, to develop its own security program template for reviewing and assessing the information security programs of service providers. But the 20 CIS Controls may be a ready tool to approach these assessments for any service provider. You may be able to use them as the framework for your reviews.

3. **Focus on core functions.**

Along the same lines, go for assessment of whether the service provider's security program effectively addresses at least core functions. The six core functions identified by NYDFS in its Cybersecurity Regulations again are:

- Identify and assess cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's information systems
- Use defensive infrastructure and implement policies and procedures to protect information systems and Nonpublic Information from unauthorized access, disruptions and misuse
- Detect attempts at unauthorized access, disruption or misuse
- Respond to such attempts to mitigate any negative effects
- Recover from such events and restore normal operations and services; and
- Fulfill regulatory reporting requirements.

One may want to adjust the list of core functions to meet your company's highest security concerns, but the foregoing list of core functions is a handy start for evaluating the components of a service provider's security program. If any core function is missing, you need to probe further.

4. **Take a broad view of what information must be protected by the service provider's security program.**

We have historically focused too much on narrow definitions of "Nonpublic Personal Information" in our security reviews and related contractual commitments for security controls. While the definition of "Confidential Information" in the confidentiality clause of the agreement is almost always broad, when it comes time to negotiating the scope of your company's information protected by contractual security plan commitments, service providers have often pushed back to make commitments only for the legal minimum. We should be moving to a broader definition of what information must be protected by the service provider's security program, including for what security events trigger notification to your company. Consistent with the NYDFS Cybersecurity Regulations, consider seeking protection of all nonpublic information, even if (i) it is business-related and not personally identifiable if it when accessed could cause material adverse impact to your company; (ii) the information when combined with other information (even though not part of the services) could be used to personally identify an individual; and (iii) any type of health-related information derived from any source.

- Focus on protecting any type of information that when

  accessed on an unauthorized basis could cause material adverse impact to your company.

- Focus on protecting any data elements about individuals, even if the data set shared with the service provider does not in itself constitute personally identifiable information, on the assumption that if the data are disclosed, they could be combined with other accessible information to identify the individual.

- Think broadly about (and document as contractual commitments) what information security events occurring with the service provider need to be promptly reported to you as service recipient – notification for all events involving all protected information (as broadly defined).

- Get tough on security incidents. Include dramatically escalated contractual remedies for security events if the incident could have had a reasonable likelihood of materially harming parts of your company's operations. Security incidents of this nature must be grounds for service provider undertaking remediation actions at its own expense, but they should also be grounds

for material breach of the contract with damages even if the harm doesn't eventually occur. The risk that the harm could have occurred is enough to warrant the right for the service provider to terminate the contract for cause for security events that could have materially harmed your company.

5. **Have your company develop its own preferred tool for security/ cybersecurity assessment of its service providers.**

   The FFIEC Cybersecurity Assessment Tool may be most valuable to financial institutions, but it reminds us that cybersecurity assessments can be broken into parts and analyzed by categories and ranked at levels. Consider the FFIEC Tool's two parts: Inherent Risk Profile and Cybersecurity Maturity.

   - An Inherent Risk Profile can be created to identify the service provider's inherent risk before implementing controls.
     - First assesses the service provider's inherent risk profile based on key categories. The FFIEC tool uses these 5 key categories, but your company may develop others:
       - Technologies and Connection Types
       - Delivery Channels
       - Online/Mobile Products and Technology Services
       - Organizational Characteristics
       - External Threats
     - The inherent risks identified are ranked with risk levels (e.g., least inherent risk, minimal inherent risk, moderate inherent risk, significant inherent risk, and most inherent risk).
   - The Cybersecurity Maturity includes domains, assessment factors, components, etc. across key maturity levels to identify specific controls and practices that are in place. The service provider's Cybersecurity Maturity level can be evaluated across each of identified key domains. The FFIEC tool uses these 5 domains, but your company can identify others:
     - Cyber Risk Management and Oversight
     - Threat Intelligence and Collaboration
     - Cybersecurity Controls

        - External Dependency Management
        - Cyber Incident Management and Resilience
    - The maturity level can then be defined (e.g., baseline, evolving, intermediate, advanced, and innovative).
- An assessment tool can be used to provide a measurable and repeatable process to assess the service provider's level of cybersecurity risk and preparedness.

6. **Develop a strong set of written policies and procedures addressing security concerns associated with your third party service providers with access to your nonpublic information.**

   Documentation of policies and procedures is a valuable form of control and, for that reason, the NYDFS and other regulators emphasize this. Documentation of the policies and procedures may be time-consuming and involve many stakeholders within your company, but once done, they will provide a roadmap for your business and vendor management teams to follow and your auditors to test against.

   The policies should include, to the extent applicable:

   - Identification and risk assessments of third party service providers
   - Minimum cybersecurity practices required to be met by such third party service providers
   - Due diligence processes to evaluate the adequacy of such third party service providers' cybersecurity practices
   - Periodic assessment of the service providers based on the risk they present and the continued adequacy of their cybersecurity practices
   - Relevant guidelines for due diligence or contractual protections relating to third party service providers including those addressing:
     - The service provider's policies and procedures for access controls (e.g., use of multi-factor authentication or risk-based authentication)
     - The service provider's policies and procedures for use of encryption or its security alternatives
     - Security breach notification requirements

- Representations and warranties addressing the service provider's cybersecurity policies and procedures that relate to the security of the your company's information systems or Nonpublic Information

7. **Invest in an adequate management and recordkeeping system for all contemplated documentation and records related to oversight of your third party service providers.**

   The regulatory developments advocate for substantial due diligence, risk assessments, contractual protections, required reporting, periodic reviews, audit reviews, related policies and procedures, etc. for oversight of your third party service contracts. It is a lot of documentation! Chances are that the system your company developed some years ago for tracking and storing this information is not up to current needs.

   - Invest in an adequate centralized storage and retrieval system, well-indexed with useful search functions, that can be accessed by key stakeholders on a need to know basis, such as your teams from Contracts Negotiation, Third Party Risk Management, Legal, Compliance, Finance, etc.
   - If the repository system is too hard to navigate and retrieve documents, team member may divert documentation to other libraries.
   - You will need controls and checks in place to make sure that all final documents that need to get deposited to the centralized system do in fact get deposited there. "Where are the executed versions of the last five amendments to that contract?"

8. **Size matters.**

   The Proposed Interagency Regulatory Rules on Enhanced Cyber Risk Management Systems remind us that "Size matters!" Enhanced cybersecurity standards for large interconnected firms is most applicable to the financial services industry, but the takeaway here for the rest of us is that the larger your service provider is and the more data shared with it, the more likely that a significant security breach of the service provider will have larger impact on your company with ripple effects on your clients, business partners and other companies in your industry sector. The scale and scope of the related risks need to be addressed through the controls you impose on the large service provider through contractual commitments and through escalated reporting and monitoring requirements.

9. **Treat your affiliates as third parties. If your service provider is actually an affiliate of your company, as a general matter, you should approach the affiliate on an arm's length basis, seeking the same protective standards, terms and conditions in the service transaction as you would require from an unaffiliated third party.**

   Financial institutions are subject to express restrictions on their transactions with affiliates[7] that require insured institutions to subject transactions with their affiliates to the same standards, terms and conditions they would get in comparable transactions with unaffiliated third parties. Although these regulatory restrictions are harsh and designed to protect the insured institution from abuse by the affiliate, outside the financial services world it is still a best practice to approach transactions with affiliates on an arm's length basis, subject the affiliate to comparable due diligence, risk assessment, contractual terms and oversight program as your company would pursue for service transactions with unaffiliated third parties. Don't be casual about business transactions with your affiliates.

   - It is true that your company will have better knowledge about the affiliate and is less likely to sue or be sued by the affiliate. However, it would be a mistake to not document a formal diligence review and risk assessment on the affiliate service provider. They may point to vulnerabilities you were unaware of and specific risks that require protective contractual commitments and other controls. In the event of a significant breach, it may look irresponsible, both financially and from your customers' viewpoint, if your company failed to sufficiently negotiate and document an adequate contractual arrangement with the affiliated service provider.
   - Although a law suit among affiliated entities may be unlikely, in the event of trouble, payment of damages and exercise of indemnification rights may be necessary. Regulators, shareholders, auditors and other parties may expect that if your affiliate's significant security breach causes your company material harm, the affiliate should make your company whole for all damages pursuant to well-developed contractual requirements.

---

7. See, for example, Regulation W, 12 CFR Part 223.

- Tax transfer pricing requirements, local law requirements and appropriate governance structures observing the separate identities of different legal entities may require that your company treat the affiliate in a comparable manner that it would an unaffiliated third party.

10. **Be sure to analyze all the risks and work through what additional and/or tailored controls should be applied to special service arrangements.**

    One size does not fit all in the service relationships. Part of the benefits of conducting due diligence and risk assessment is to understand and weight the vulnerabilities of a given relationship. Different types of service relationships present their own unique risks. Two types of special service relationships are discussed below.

    - **Managed Security Service Providers**. As security issues have become more demanding for companies with increasingly sophisticated threats and as regulatory and industry standards proliferate, faced with mounting cost pressures and a shortage of internal expertise, some companies have turned to partially or completely outsourcing their security functions to third party service providers, sometimes known as Managed Security Service Providers ("MSSPs"). The types of services offered by MSSPs include network boundary protection; management of intrusion detection and prevention for networks and hosts; event log management and alerting; anti-virus and web content filtering services; patch management and security software management; security incident response and management; data leak protection; secure messaging, etc.
        - The MSSP arrangements present particular risk management issues related to loss of control of the outsourced security function. Increased risk may arise from poor planning, lack of oversight and control, and/or poor MSSP service performance.[8]

8. For more information, see http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/appendix-d-managed-security-service-providers.aspx.

- Before outsourcing security functions in whole or part with an MSSP, your company should consider at least the following risks associated with MSSP relationships and develop counterbalancing controls against the risks:
  - Decline in business reputation and customer confidence if service problems arise
  - Liability under customer agreements
  - False sense of security the outsourcing may give your company's management
  - Diverse offshore (if applicable and it frequently is) legal, geopolitical and cultural risks
  - Impact on competitive advantage if valuable intellectual property or proprietary information is stolen
  - Reputational damage should the MSSP fail to provide the contracted service
  - Heightened legal and regulatory issues
  - Instability to the service relationship related to change in the financial condition of the MSSP
  - And perhaps the most critical risk, dependence on an outside organization for critical services, with the related loss of internal experience, knowledge and skill development.

- **Cloud Relationships.** Companies are increasingly contracting with cloud service providers for a variety of service needs. Cloud relationships are another type of outsourcing, but one where the company relocates its resources such as data, applications, and services to computing facilities outside the company's corporate firewall, which the user then accesses via the Internet. Cloud computing is a migration from owned resources to shared resources in which the user receives information technology services on demand from the third party service provider through the Internet "cloud." The service deployment model may take the form of private clouds (operated solely for the company) or public clouds (services available to any paying customer), or some variation in between (e.g., a community cloud shared by several companies). The benefits of cloud services may

include cost reduction, flexibility, scalability, improved load balancing and speed.

The risks associated with the particular cloud computing arrangement needs to be carefully vetted during the due diligence process. Issues to review may include:[9]

- Data classification: How sensitive is the data that will be placed in the cloud and what controls are in place to ensure the data is properly protected?
- Data segregation: Will the company's data share resources with data from other cloud clients? E.g., will the data be transmitted over the same networks or be stored or processed on servers that are used also by other clients?
- Recoverability: How will the service provider respond to disasters and ensure continued service?
- Will the cloud provider commit to complying with the data security regulatory standards to which the company is subject? (Many cloud providers want to offer their service with fixed contractual commitments as a "service bureau.")
- Will the cloud provider commit to strict restrictions on disclosing or using or reusing the company's data for purposes other than performance of the cloud services?
- Does the cloud provider have adequately documented plans and resources to continue operations if unexpected disruptions occur?
- When terminating the relationship, is the underlying contract clear on the ownership, locations, and formats of the data? Is it clear that the cloud provider is able to remove the company's data from all locations where it is stored?
- Are the company's auditors able to effectively access the cloud provider's internal controls?
- Does the particular cloud deployment model increase the frequency and complexity of security incidents? If so, is the company able to respond by increased monitoring of

9. For additional information, see, http://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.

security-related threats to the networks and generally to ensure that the cloud provider is maintaining effective controls?

- If the data is stored or processed outside the U.S., the company will need to attain an understanding of what non-U.S. laws may impede the ability of the company to control access to its data and meets its responsibilities under various U.S. laws to respond to and report security incidents, respond to service of process and regulatory demands, comply with consumer privacy and protection laws, etc.

APPENDIX C

TOP TEN TIPS FOR CONTROLLING PRIVACY AND CYBER-SECURITY RISKS IN THIRD PARTY SERVICE PROVIDER TRANSACTIONS (excerpt from 2018 presentation)

1. **Develop contractual commitments, including security standards, on the assumption that security standards and related compliance expectations will need to change, in the expectation of increasing controls and more diverse security requirements.**

    - Although many in the public sector have talked about rationalization of, or harmonization under, a common cyber security framework, one should assume that we will continue to operate in the US under a hodgepodge of laws, regulations and case law, presenting competing concepts of what constitutes reasonable and baseline security standards and creating varied compliance obligations.

2. **Enhance your company's corporate and organizational governance framework with respect to oversight of third party service providers.**

    - A company's deployment of appropriate corporate and organizational governance framework to oversee cybersecurity risks and support decision making based on the company's risk appetite, including for making adequate cybersecurity disclosures, is gaining increasing regulatory attention.

3. **Make measurable enhancements to your company's cyber resiliency to third party vendor security incidents.**

    - As cyberattacks continue to grow in number, size and sophistication, it is necessary for companies to make measureable enhancements to their cybersecurity resiliency. Measureable enhancements to cybersecurity resiliency require deployment of enhanced controls, more accurate metrics, and attainment of better risk management data about your third party service providers.

4. **Enhance your vendor due diligence processes.**

    - Many companies have not updated their due diligence questionnaires for vendors in years, although cyber threats have continued to multiple and new lessons can be learned from different security breaches. Consider incorporating some automated due

diligence assessment tools to improve your data collection and facilitate periodic updating of the questionnaire responses.

5. **Further assess your service provider's Inherent Risk Profile and include in the contract specific controls directed at those risks.**

   - We are inadvertently developing more target rich environments for cybercriminals with the assistance of vendors through creation of new platforms and digital and mobile channels designed to improve customer experience and expansion of the Internet of Things, but these developments have a tendency to increase the potential for more vulnerable connections and high risk fraud losses related to online account takeovers.

6. **Reassess the strength of your company's offshore vendor management program.**

   - Companies remain under increasing pressure to cut expenses by using service providers in lower cost jurisdictions. But using third party vendors in jurisdictions with laws, policies, and risks that are different from those of the United States poses threats to your company's operations. Many companies have not updated their offshore vendor management programs in many years. Are procedures in place for regularly testing data integrity and vulnerabilities? Are the established data access controls being enforced?

7. **The outsourcing of security services to third parties must be particularly assessed thoroughly, well-documented and well-managed.**

   - Corporate pressures to cut expenses and seek efficiencies has led to an increasing number of security-related services being outsourced to managed security service providers ("MSSPs") and other vendors. At the same time, regulators are closely scrutinizing companies' reliance on third party service providers to meet their cybersecurity needs and obligations.

8. **Assess the effectiveness of your ongoing monitoring program of vendors and where deficiencies are noted, make enhancements.**

   - Is the vendor making the required reporting? Does your company review and assess all the information the vendor is required to report? Has your company identified gaps where new reporting is needed? Do the respective service managers meet regularly, thoroughly reviewing service level performance

and incident response data? Is the original due diligence data updated and reassessed annually, and also in response to particular developments?

9. **Take great care to negotiate sufficient audit right provisions in the contract.**

    - Because of vendor push-back, companies often back off the scope of audit rights they originally requested. Although it may be acceptable for lower risk vendors to simply provide your company with copies of their SSAE 18 audit reports, for higher risk vendors, it is important for your company to obtain the right to conduct regular on-site reviews and audits of the vendor's operations and security program.

10. **Test to ensure your vendor's security remediations are effective.**

    - Although it is important to obtain prompt reporting of security incidents from your vendors and cooperation after discovery of the breach, assessment and validation of the effectiveness of your vendor's remediations after the security incident is critical.

NOTES

31

Mayer Brown Cybersecurity and Data Privacy Update

Submitted by:
Rebecca Eisner
Mayer Brown LLP

Table of Contents

EU CYBER THREAT LANDSCAPE AND OUTLOOK: WHAT YOU SHOULD KNOW ABOUT THE ENISA 2018 REPORT 5
Cyber Threat Landscape in 2018: More of the Same and One New Joiner 5
In 2019, Organizations Should Pursue a Cybersecurity Strategy 7
2019 OUTLOOK – CYBERSECURITY DATA PRIVACY 9
Key Issues 9
Managing Cyber Incidents Across Borders 10
Cross-border cyber incidents are likely to become more frequent in 2019 10
Continued Regulatory Pressure on Cybersecurity and Data Privacy 13
Expanding Cybersecurity and Data Privacy Litigation 17
Increasing Adoption of Comprehensive Data Privacy Regimes 20
Focus on Data Privacy and Cybersecurity Policy 23
Conclusion 26
Contributors 29
KEEPING IT PRIVATE: GDPR AND DEVELOPMENTS IN DATA PRIVACY IN 2018 31
The General Data Privacy Regulation 32
The California Consumer Privacy Act and the Consequences of GDPR in the United States 34
Likely Effects of GDPR in 2019 and Beyond 35
TOP TIPS: PREPARING TECHNOLOGY ARRANGEMENTS FOR BREXIT 37
DOJ RELEASES UPDATED CYBER INCIDENT RESPONSE GUIDANCE FOR PRIVATE SECTOR ENTITIES 42
Steps to Take Before a Cyber Intrusion or Attack Occurs 42
Responding to a Cyber Incident: Executing Your Incident Response Plan 44
What Not to Do Following a Cyber Incident 45
What to Do After a Cyber Incident Appears to Be Resolved 46
Conclusion 46
CALIFORNIA ENACTS FIRST STATE LAW TARGETING IOT CYBERSECURITY 47
5 CONSIDERATIONS FOR GENERAL COUNSELS REGARDING THE NEW YORK CYBERSECURITY REGULATIONS 50
Annual Board Report and Certification 50
Breach Notification 51
Third-party Service Provider Compliance 51
Data Governance and Classification 52
Training 52
Be Aware of New State Cybersecurity Requirements 53

CALIFORNIA ENACTS GDPR-LIKE CONSUMER PRIVACY PROTECTIONS: WHAT YOU NEED TO KNOW 54
Coverage of the CCPA 54
Key Components of the CCPA 55
ePRIVACY REGULATION: WHAT TO EXPECT (AND WHEN) OR WHY DOES IT TAKE TWO (OR EVEN THREE) TO TANGO? 60
Progress Report 60
Statement of the EDPB 61
What's Next (and When)? 62
INTERNATIONAL DEVELOPMENTS IN PRIVACY LAWS AND VENDOR AGREEMENTS 63
Developments in the United States 63
Developments in the European Union 64
Developments in the Asia-Pacific Region 65
Updates to Vendor Contracts 67

EU CYBER THREAT LANDSCAPE AND OUTLOOK: WHAT YOU SHOULD KNOW ABOUT THE ENISA 2018 REPORT

6 February 2019

Mayer Brown Legal Update

The landscape for cyberattacks is constantly evolving. Attacks are becoming more global and sophisticated, and 2019 is poised to continue this trend toward increasing complexity.

This Legal Update highlights: (i) the main aspects of the threat landscape identified by the European Union Agency for Network and Information Security ("ENISA") in its 2018 Threat Landscape Report (the "Report") published on January 28, 2019, and (ii) the recommendations from ENISA for businesses to increase resilience and foster improved cybersecurity in 2019. Set up in 2004, ENISA is contributing to a high level of network and information security ("NIS") within the European Union and working to develop a culture of NIS, and raise awareness, in society. Its yearly edition of the Report contributes to the identification of the cyber threat landscape and supports the development and implementation of the European Union's policy on matters relating to NIS.

For a more global perspective on cybersecurity and privacy outlook, please read the *2019 Cybersecurity and Data Privacy Outlook*.

Cyber Threat Landscape in 2018: More of the Same and One New Joiner

The Report identifies the top 15 cybersecurity threats in Europe. The top four threats remain unchanged compared to the previous year: (1) malware, (2) web-based attacks, (3) web-application attacks and (4) targeted forms of phishing (in that order). Meanwhile, denial of service ("DoS") botnets and data breaches increased in 2018. The Report also found a new threat: "cryptojacking." We discuss some of the Report's findings below.

- DoS attacks, and especially distributed DoS ("DDoS") attacks, are an impactful threat in the cyber landscape and have been used to target businesses across economic sectors. Defending against this type of threat (notably by hiring dedicated vendors) has become a central challenge for the private sector with financial services, e-commerce companies, cloud providers and governments devoting

significant resources to the issue.[1] Research suggests that the number of DDoS activities is on the rise (a 16-percent increase in summer 2018 when compared to the same period in 2017).[2] Although law enforcement activities have challenged this breed of malicious cyber activity, the Report noted that the increase in the number of connected services globally and their dependency on the Internet of things (IoT) increase the threat of DoS and other types of attacks. As connectivity grows, such attacks have the potential to cause systemic failure for businesses and critical systems (e.g., in connected hospitals and related services).

- The Report noted that, during 2018, botnets were active and used to advance various malicious activities. For example, the Report revealed that 88 percent of spam was found to have originated from botnets and new botnets have been developed around IoT, social media and online advertisements. The Mirai malware technique (and source code) inspired criminals to build even more sophisticated IoT botnets (Tori-bot, a prominent type of botnet identified in the Report, has six persistency techniques targeting multiple architectures.)
- The Report noted that data breaches (incidents leading to the alteration, compromise or loss of data) have affected significantly more records in 2018,[3] with the average cost of breach increasing by 6.4 percent. The introduction of a more comprehensive data breach framework in the European Union (since the entry into force of GDPR) could explain some of that increase. Social media platforms account for a majority (56 percent) of reported breaches, and some industry sectors (e.g., healthcare, 27 percent) have been particularly vulnerable. The Report found that 48 percent of breaches were caused by external attackers first, while human error and negligence, along with technical error, accounted for 27 percent and 25 percent, respectively.

---

1. See the Arbor network report (https://pages.arbornetworks.com/rs/082-kna-087/images/12th_worldwide_infrastructure_security_report.pdf).
2. See https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf.
3. 4.5 billion data files were breached worldwide in the first half of 2018, up from 2.7 billion in the same period of 2017, according to the data breach index cited in the Report.

- According to the Report, 2018 was the year of cryptojacking, a phenomenon appearing among the top 15 threats for the first time. Cryptojackers use the victim's computer power to "mine" cryptocurrencies, such as Bitcoin or Monero, without the victim's consent. Higher profits have driven cybercriminals to focus on cryptojacking. The implementation of content filtering that screens out suspected cryptojacking software in emails and employs regular security audits should, according to the Report, help to detect anomalies in the usage of computer power linked to cryptojacking.

In 2019, Organizations Should Pursue a Cybersecurity Strategy

Throughout the Report, ENISA identified specific measures that could be adopted in the business context to minimize risks to cybersecurity. According to the Report, recommended steps in the development of a cybersecurity strategy include the following:

- **Estimate risks from cyber threats, or "know your enemy" (and yourself)**. Businesses should assess the potential impacts of a successful cyberattack on their assets and customer base and adopt the required security measures. Risk assessment should take into account the evolution of cyber threats, particularly the growing focus on automated attacks and attacks on mobile devices and IoT.
- **Define cyber threat intelligence ("CTI") processes**. Collection and analysis of CTI contributes to a better understanding of the motives and techniques used to conduct a cyberattack (and the ability to anticipate potential damage).
- **Share CTI with other stakeholders**. Sharing CTI can help facilitate the identification of common threats, as well as best practices and effective security measures (eventually at a sector-specific level). Existing CTI networks should be enlarged, and the volume of CTI shared should be increased.
- **Consider supply chain threats**. In complex product development processes, threats affecting different levels of the supply chain can have a cascading effect that ultimately impacts the end user. Coordinated action at a sector-specific level should ensure a common approach to these systemic threats. In addition, relying on certification at every stage of the supply chain may help to facilitate end-to-end security.

In all of these aspects, the role of ENISA is set to increase in 2019 following the adoption of the EU Cybersecurity Act. The Cybersecurity Act[4] paves the way for EU cybersecurity certification schemes for ICT products (i.e., hardware and software elements of network and information systems); services (i.e., services involved in transmitting, storing, retrieving or processing information via network and information systems); and processes (i.e., sets of activities performed to design, develop, deliver and maintain ICT products and services). Since 2019 is the first full year since the adoption of the NIS framework by EU member states, cybersecurity awareness will be a key consideration for businesses operating in the European Union.

Indeed, cybersecurity is likely to stand among the most significant challenges that multinational businesses must address in 2019. Businesses will benefit from continuing to refine their cyber risk management and data privacy compliance programs to address the evolving EU cyber regulatory landscape in the coming year.

4. For previous coverage on the Cybersecurity Act, see here.

Key Issues

Managing Cyber Incidents Across Borders

Continued Regulatory Pressure on Cybersecurity and Data Privacy

Expanding Cybersecurity and Data Privacy Litigation

Increasing Adoption of Comprehensive Data Privacy Regimes

Focus on Data Privacy and Cybersecurity Policy

Cybersecurity and data privacy presented some of the most complex legal questions and business risks that multinational companies faced in 2018. Businesses should expect continued growth in cyber and data privacy challenges in 2019.

Cyber attacks became even more sophisticated and severe in 2018, with incidents ranging from exfiltration and extortion schemes, to attacks on critical infrastructure, threats to connected products, and vast data breaches. Even technically simple (but often highly costly) business email compromise attacks spiked in 2018, underscoring the continuing importance of implementing defensive best practices. The data privacy landscape also continued to grow more complex, as the General Data Protection Regulation ("GDPR") went into force in the European Union ("EU")—and affected business practices around the globe. Other jurisdictions are already following suit, passing similar laws that will require significant compliance efforts.

2019 is poised to continue this trend of increasing complexity—and consequences—for cybersecurity and data privacy challenges. The adoption and new use cases for disruptive technologies—whether autonomous vehicles, artificial intelligence, connected products or much more—will help drive the evolution of the cybersecurity and data privacy legal landscape, along with the introduction of new regulatory regimes, expanding litigation risk and scrutiny from policy makers across jurisdictions.

The stakes are high. A report issued by the White House Council of Economic Advisers in 2018 estimated that malicious cyber activity cost the US economy between $57 billion and $109 billion in 2016 alone. For individual companies, the effects can be devastating. Cyber incidents have led to the departure of companies' most senior executives, disrupted mergers and acquisitions, and caused massive financial and reputational costs. Data privacy compliance issues have resulted in

both substantial legal penalties and loss of the consumer trust on which companies depend.

Against this background, key cybersecurity and data privacy issues for multinational companies in 2019 will include:

- Managing Cyber Incidents Across Borders
- Continued Regulatory Pressure on Cybersecurity and Data Privacy
- Expanding Cybersecurity and Data Privacy Litigation
- Increasing Adoption of Comprehensive Data Privacy Regimes
- Focus on Data Privacy and Cybersecurity Policy

Managing Cyber Incidents Across Borders

Recent years have seen steady growth in the sophistication and severity of cyber attacks on multinational businesses. Increasingly, these incidents are not limited to a single jurisdiction, but stretch across borders, often in a manner that makes responding to the incident substantially more complex. A breach of a customer database, for example, may trigger notification obligations in multiple countries, and a ransomware attack may encrypt systems across a company's global footprint. Similarly, a forensic investigation may require a company to act across borders, such as by working with third-party hosting companies in different countries. Moreover, cyber incidents involving connected products may affect multiple jurisdictions at once for any company that sells into multiple markets. In these and many other cases, the cross-border nature of the incident can make responding significantly more complicated, whether because of competing regulatory imperatives and legal risks in different jurisdictions, increased challenges coordinating actions across globally distributed teams, or practical obstacles in reaching affected systems.

Cross-border cyber incidents are likely to become more frequent in 2019

Here, we identify key issues that companies may face in responding to these incidents—and that companies will likely benefit from thinking through and addressing in relevant incident response plans and playbooks in advance.

Managing Forensic Investigations on a Global Basis. Performing an effective forensic investigation on a global basis can substantially reduce legal risk in the wake of a cyber incident that crosses borders. Managing the investigation so that key artifacts are secured, appropriate analyses are performed in a timely manner, and sound conclusions are reached using a documented methodology, can position a company well for potential litigation, enable it to interact more confidently with regulators, and support more effective engagement with law enforcement. For example, a sound forensic investigation (and a proper understanding of the confidence that should be laid upon findings) can help to determine which geographic regions may be affected by a data breach and what data may have been rendered unavailable, corrupted or subject to unauthorized access or loss. As data privacy regimes continue to expand and develop in 2019, answering such questions is likely to be essential to effectively navigating legal and regulatory obligations—including individual and regulatory notification requirements—that may have been triggered by such an incident.

Managing Legal Risk on a Global Basis. Cross-border cyber incidents can raise legal questions under the laws of numerous jurisdictions, including some in which the affected company may not routinely do business. Consequently, the coming year is likely to see companies facing pressure to manage the geographically and substantively diverse legal issues raised by cross-border incidents. In responding to this challenge, companies are likely to want to ensure not only that they have sufficient capability to understand the laws in these various jurisdictions, but also that they can effectively manage competing legal interests across jurisdictions. For example, in the United States, companies responding to an incident will often issue a broad litigation hold to avoid deletion of data that is likely to be relevant to anticipated litigation. However, this can sometimes come into tension with privacy laws in other jurisdictions that direct the deletion of data that is no longer required for business purposes. In addition, regulatory and public expectations for prompt notifications and transparency and views on appropriate levels of inquiry may vary across borders. Such variation makes it likely that companies will face challenges in balancing the need to communicate with regulators and other stakeholders with other legal risks, including potential litigation in the United States.

Strategic Law Enforcement Engagement. Because crossborder cyber incidents often involve criminal activity in multiple jurisdictions, companies will likely find themselves balancing the risks and benefits of

engaging with one or more law enforcement agencies as part of their incident response processes. Engaging with law enforcement in a cross-border incident can be a prudent step. Law enforcement agencies can provide threat intelligence, coordinate with foreign counterparts to compel third-party disclosures, or take steps, such as seizing servers used by malicious actors, that may mitigate harm or deter the threat actor from taking further damaging actions. However, law enforcement engagement also can come with trade-offs, including the potential loss of control and confidentiality over specific aspects of an incident response process. Analyzing these potential costs and benefits can be particularly complex in the context of a cross-border incident that can implicate the interests of law enforcement agencies in multiple countries. For example, a company may have to decide which law enforcement agency or agencies it should engage with, how this decision will impact engagement with regulators in those countries, and how it will support any ongoing engagement with foreign law enforcement.

Preserving Privilege. Many countries recognize some form of attorney-client privilege, but the protection varies in its application and scope even where it is recognized. For example, some countries do not provide in-house counsel work product and communications the same level of protection often afforded to those of outside counsel, and privilege can be lost if information is communicated to wider groups of recipients within a client. Understanding these jurisdictional distinctions is likely to be important as companies respond to cross-border incidents and manage subsequent regulatory inquiries or civil discovery. Moreover, companies facing such incidents in 2019 are likely to benefit from following standard best practices for protecting privilege where it applies, including by employing appropriate markings on all documents and keeping communications to "need to know" audiences within the business.

Extraterritorial Application of Data Privacy and Security Laws. Various data privacy and security laws extend to businesses based well beyond a country's borders. For example, the GDPR applies to data processing activities relating to the offering of goods or services to data subjects situated in the EU and monitoring of the behavior of such data subjects, even if the business is not formally established in the EU. Companies facing cross-border incidents in 2019, consequently, will want to evaluate the full range of legal regimes to which they may be subject and which supervisory authorities they will be required to coordinate with.

Continued Regulatory Pressure on Cybersecurity and Data Privacy

Regulatory scrutiny of cybersecurity and data privacy practices continued to grow across industries in 2018. We expect regulators to continue this trend in 2019 through use of the full range of regulatory tools, including new or updated guidance, investigations and enforcement actions, engagement with industry and other stakeholders, supervisory examinations and public education. This trend will likely be seen across numerous economic sectors. We focus below on five areas—financial services, public company disclosures, medical devices, connected vehicles, and consumer data security and privacy—that are likely to see regulatory activity in the coming year, both with respect to traditional enterprise technology and the expanding world of connected products.

FINANCIAL SERVICES

Financial services regulators have long taken a leading role with respect to cybersecurity and data privacy. 2018 was no exception as a broad range of state and federal agencies engaged with industry on these important topics. This trend is set to continue into 2019.

Financial institutions and other public companies will benefit from carefully monitoring proposed regulatory changes both to take available opportunities to weigh in and shape regulatory policy and to enable effective compliance. Below we highlight regulatory topics for financial services companies and institutions to watch in 2019.

NAIC Model Data Security Law Implementation. In May 2018, South Carolina became the first state to adopt the model data security law that was developed in 2017 by the National Association of Insurance Commissioners ("NAIC"). In December 2018, Ohio and Michigan became the second and third states to adopt the NAIC model law. If adopted by a state, the NAIC model law will build on existing data privacy and consumer breach notification obligations by requiring insurance licensees to comply with detailed requirements regarding maintenance of an information security program and notification of cybersecurity events. We expect that more states will adopt the NAIC model law in 2019, with versions already introduced in the Rhode Island and Nevada legislatures.

NASAA Model Information Security Rule Proposal. In September 2018, the North American Securities Administrators Association ("NASAA") proposed a model rule for information security and privacy requirements for state-registered investment advisers

("state-RIAs"). We expect the proposal will be finalized in 2019, but it remains to be seen how rapidly it will be adopted by states, and it is unclear how the proposal will interact with existing cybersecurity requirements, such as Colorado's and Vermont's cybersecurity regulations for broker-dealers and state-RIAs providing services in those states or Massachusetts's generally applicable cybersecurity regulation.

New York Cybersecurity Regulation Implementation. The cybersecurity regulation ("NY Regs") adopted by the New York State Department of Financial Services will turn two years old in February 2019, and the final requirement in its phased implementation schedule will become effective in March 2019. This final requirement relates to the relationship between financial institutions that are authorized to engage in business in New York ("Covered Entities") and third-party service providers ("TSPs"), and will require Covered Entities to pass on certain cybersecurity obligations to TSPs by requiring Covered Entities to develop written policies and procedures designed to ensure the security of systems and data accessible to, or held by, TSPs. Additionally, each Covered Entity will be required to address with their TSPs, through due diligence or contractual protections, (i) the use of access controls and multifactor authentication, (ii) encryption of nonpublic information in transit and at rest, (iii) prompt notification to the Covered Entity of certain cybersecurity events and (iv) representations and warranties from the TSPs concerning their cybersecurity policies and procedures.

SEC Red Flags Rule Enforcement. In September 2018, the US Securities and Exchange Commission ("SEC") brought its first enforcement action against a registered broker-dealer/investment adviser under the Identity Theft Red Flags Rule ("Regulation S-ID"). While this is the SEC's first enforcement action alleging violations of Regulation S-ID, it is part of a growing trend of initiatives by the SEC and the Financial Industry Regulatory Authority that focus on cybersecurity in their examinations of registered securities entities.

NFA Breach Notification Requirement. In January 2019, the National Futures Association ("NFA") revised the information security requirements for its members, which consist largely of regulated participants in the commodity derivatives markets. The revisions become effective on April 1, 2019, and require members to notify the NFA of a breach, similar to the regulator notifications required under the NY Regs.

US Treasury Department Critical Infrastructure Initiative. In July 2018, the US Department of the Treasury released a report "identifying improvements to the regulatory landscape that will better support nonbank financial institutions, embrace financial technology, and foster innovation." The Treasury Department used the report to announce that it will lead "a multiyear program with the financial services industry to identify, properly protect, and remediate vulnerabilities" with respect to critical infrastructure. We expect further details on this critical infrastructure initiative to be released in 2019.

PUBLIC COMPANY DISCLOSURES

In February 2018, the SEC highlighted cybersecurity concerns for public companies by formalizing guidance that reiterates that companies should consider the materiality of cybersecurity risks and incidents when preparing required disclosures. In addition, the revised guidance addresses the importance of policies and procedures related to cybersecurity by encouraging companies "to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure." Going forward, public companies across industries are likely to continue to face challenging questions regarding potential disclosure obligations under this guidance. Moreover, because cybersecurity risks and incidents may qualify as material nonpublic information, companies will want to pay attention to the SEC's guidance on evaluating and monitoring trading activities to avoid potential insider trading exposure. In several high-profile data breaches, senior company officials have faced intense scrutiny for trading activity that appeared to be based on insider information, and the SEC appears poised to continue this trend in 2019.

MEDICAL DEVICES

The US Food and Drug Administration ("FDA") continues to prioritize cybersecurity of medical devices and made significant headway on promised cybersecurity activities in 2018. We expect that trend to continue into 2019 as FDA continues to push these initiatives into action. Although FDA typically does not update guidance on a periodic basis, in October 2018, FDA issued draft guidance that, once final, will supersede the October 2014 final guidance on the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Public meetings to solicit comments on the draft guidance are scheduled for January 2019, and FDA will likely move quickly on finalizing the guidance after the comment period closes in March. Most

notably, the new draft guidance focuses on how manufacturers can address the risks to patient safety created by connected devices. FDA also made efforts to facilitate increased information sharing across the federal government in the coming years by signing a Memorandum of Understanding with the Department of

Homeland Security to further increase cooperation between the agencies, and by creating two new Information Sharing and Analysis Organizations. Finally, in 2019, health care delivery organizations have a new tool to respond to cybersecurity incidents in the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, sponsored by FDA.

CONNECTED VEHICLES

The Department of Transportation ("DOT") and the National Highway Traffic Safety Administration ("NHTSA") have prioritized cybersecurity in recent years, including through ongoing engagement with industry stakeholders and the issuance of Cybersecurity Best Practices for Modern Vehicles in October 2016. In the past year, DOT continued to highlight cybersecurity and data privacy as key topics for companies to address as they build automated driving systems. Its guidance document, Preparing for the Future of Transportation: Automated Vehicles 3.0 ("AV 3.0"), issued in October 2018, built upon DOT's last major statement addressing automated vehicles: Automated Driving Systems 2.0: A Vision for Safety ("A Vision for Safety"), released in September 2017. A Vision for Safety identified twelve "priority safety design elements" that manufacturers were encouraged to consider in designing highly automated vehicles, including vehicle cybersecurity. AV 3.0 reaffirms this focus on cybersecurity and specifically supported the "Voluntary Safety Self-Assessment" approach announced in the 2017 policy. The new guidance noted that public-private coordination and information sharing are essential to managing cybersecurity risk and highlighted the value of engaging with the Department of Homeland Security and other public-private information sharing organizations. The continued emphasis on cybersecurity was also reflected in a September 2018 speech by the Deputy Administrator of NHTSA, who stated that "collective safety risk management through information sharing is vital" and highlighted the importance of maintaining consumer trust that the automotive industry "is committed to working together to anticipate and mitigate cyber risks." Automotive industry participants will therefore want to continue focusing on

cybersecurity and data privacy as they design, build and support increasingly connected vehicles in 2019.

CONSUMER DATA SECURITY AND PRIVACY

Enforcement activity by the Federal Trade Commission ("FTC") has been a constant feature of the consumer data security and privacy landscape over the past decade—with the commission bringing more than 60 actions alleging that companies engaged in unfair or deceptive practices that failed to adequately protect consumers' personal data. The FTC can be expected to remain focused on data security and privacy in 2019. In December 2018, the FTC held a two-day public hearing devoted to data security, at which the Director of the Bureau of Consumer Protection stated that "data security will continue to be an important priority for the FTC and that the FTC will not be retreating from its role as the nation's primary data security law enforcement agency." The FTC plans to schedule a similar public hearing on consumer privacy—"the first comprehensive re-examination of the FTC's approach to consumer privacy since 2012."

Enforcement actions are likely to remain a key tool for the FTC in 2019 as it sets consumer data security and privacy policy, including for connected devices. Many such enforcement actions may end in consent orders, but litigation also may continue to test the FTC's authority and the theories it pursues in enforcement actions. In June 2018, the US Court of Appeals for the Eleventh Circuit vacated the FTC's cease-and-desist order against LabMD, concluding that it imposed an "indeterminable standard of reasonableness" and was not specific enough in what it prohibited and what it required. 2019 may see additional challenges to the FTC's authority to bring—and ability to win—such actions, including in the FTC's litigation against a router manufacturer over allegations of inadequate security that is scheduled for trial in June.

Expanding Cybersecurity and Data Privacy Litigation

Cybersecurity and data privacy litigation continues to grow, both in the potential liability exposure it presents to companies and the types of litigation and theories advanced by plaintiffs. Countless putative privacy and cybersecurity class actions were filed in 2018, asserting claims based on federal privacy statutes, state biometrics laws and common law theories, among many other bases. Lawsuits also addressed the security and privacy implications of connected products, artificial intelligence, and other evolving technologies, and

continued to expand beyond consumer class actions. Meanwhile, courts continued to wrestle with high-stakes issues for privacy and security litigation, including the proper application of the Supreme Court's decision in Spokeo, Inc. v. Robins in this context (a question that the Supreme Court itself recently raised in a pending case) and the risk of future injury sufficient for standing in data breach cases.

Cybersecurity and data privacy litigation is poised to expand once more in 2019 as more disruptive technologies are adopted across the economy and expectations for cybersecurity and data privacy continue to evolve.

The creation of a limited private right of action under the California Consumer Privacy Act, which we discuss in more detail below, likewise suggests that this litigation will only grow over time. Companies consequently should expect litigation risk to be a key factor in determining their respective approaches to cybersecurity and data privacy in 2019 and beyond.

DATA BREACH CLASS ACTIONS

Data breach class actions remain a persistent risk for companies that hold US customers' personally identifiable information. Although litigation does not necessarily follow after every data breach, many putative class complaints continue to be filed shortly after data breaches hit the news. Following a major data breach, dozens of consumer class actions may be filed, further raising the stakes of litigation. Moreover, with close attention paid by the press and security researchers to companies' responses to incidents and plaintiffs' attorneys watching for potential missteps or failures to remediate compromised systems, litigation risks can arise well after the original compromise. Companies should therefore continue to have the management of litigation risk front of mind in responding to consumer data breaches in 2019.

It remains to be seen whether 2019 will be the year that the Supreme Court clarifies what precise risk of future harm is necessary to establish Article III standing in data breach class actions. The US Circuit Courts of Appeals are currently split on this important question, with the Third Circuit, Sixth Circuit, Seventh Circuit and DC Circuit having found the alleged risk of future harm after a data breach sufficient to establish standing, and the First Circuit, Second Circuit, Fourth Circuit and Eighth Circuit having reached contrary conclusions. This past year, the Ninth Circuit joined the former group of Courts of Appeals in its Zappos.com decision. Relying on its prior decision in

Krottner v. Starbucks Corp. (the precedential value of which had been questioned after the Supreme Court's decision in Clapper v. Amnesty International USA), the Ninth Circuit concluded that the plaintiffs' allegations of an increased risk of identity theft were sufficient to establish Article III standing. The Zappos.com petition for certiorari is pending before the Supreme Court as of the date of this publication.

INTERNET OF THINGS LITIGATION

Connected devices continue to become more deeply integrated into our daily lives and our economy. Connected cars, medical devices, toys, home appliances, consumer electronics, and more are bringing new services and capabilities to consumers. Connectivity likewise is being brought to commercial, manufacturing, agricultural, and critical infrastructure applications, from farming equipment to the factory floor and beyond. This connectivity creates exciting opportunities for companies and offers great benefits to the customers they serve.

However, these opportunities also bring new litigation risk. As anticipated, litigation relating to connected devices—often referred to as the "Internet of Things"—continued to grow in 2018. Consumers alleged that certain devices lacked adequate security and, thus, were overpriced or exposed them to a risk of future harm from cyber attacks. Other putative class actions alleged that connected devices collected or used personal data improperly, thus violating consumers' privacy rights. Ongoing litigation over automotive researchers' 2015 discovery of alleged security vulnerabilities in a connected vehicle reveals the high stakes of such litigation. In an ultimately unsuccessful petition for certiorari after class certification in that case, the defendants explained the massive potential liability at stake, describing the case as involving "three statewide classes containing more than 220,000 consumers claiming $440 million in damages." Such figures, even if only claimed at this stage, highlight the high stakes of cybersecurity and data privacy litigation regarding the Internet of Things. Indeed, this risk will only increase in the event of future cybersecurity attacks on connected devices that result in personal injury or other physical consequences.

SHAREHOLDER AND DERIVATIVE CYBER LITIGATION

Consumer class actions following cyber incidents have increasingly been accompanied by securities class actions or derivative litigation. In September 2018, for example, Yahoo! entered into an $80 million settlement of claims that the company misled investors about large-scale data breaches it suffered. Litigation also continued in 2018 in the securities class action that was filed against Equifax after it suffered

high-profile data breaches. Derivative actions have also continued. Final approval was given to a $29 million settlement of the Yahoo! data breach derivative litigation in January 2019, for example. Likewise, the fast-food company, Wendy's, settled a data breach derivative action in May 2018, with an award of almost $1 million in attorneys' fees and an agreement to take various remedial measures. Considered in combination with the reporting disclosure guidance issued by the SEC and increasing regulatory pressure on boards to perform effective cybersecurity oversight, these securities class actions and derivative actions further highlight the importance of cybersecurity and data privacy for a company's most senior leadership in 2019.

Increasing Adoption of Comprehensive Data Privacy Regimes

The implementation of the GDPR drove substantial compliance work for many companies in the past few years.

2019 is likely to see both continued focus on the GDPR as well as similar attention paid to a wave of new, GDPRlike laws that continue to complicate the data privacy landscape.

Several jurisdictions, including countries such as Brazil and states such as California, have already followed suit and passed or proposed legislation inspired by the GDPR. Managing and responding to these emerging regimes will be a key focus of private sector data privacy work in 2019.

GDPR. The GDPR came into effect in May 2018 and continues to demand significant focus by companies seeking to remain in compliance with its obligations. This regulation represented a sea change in the way privacy is regulated for individuals in the EU. Some of the key changes include:

- Direct applicability of the GDPR in the same form in all EU Member States (with some powers of derogation granted at the national level in specific areas, such as employment law);
- Expanded extraterritorial scope that captures non-EU businesses;
- Significantly higher fines of up to the higher of 4% of an enterprise's worldwide turnover or €20 million per infringement;
- New data breach notification obligations that require notice to the relevant EU supervisory authority without undue delay and where feasible within 72 hours after becoming aware of a data breach;

- New data privacy governance requirements, including the appointment of a data protection officer and the use of data protection impact assessments for higher risk processing;
- Requirement to implement "privacy by design";
- Expanded individual privacy rights, including the "right to be forgotten", the "right to data portability" and the right not to be subjected to automated data profiling; and
- New direct obligations for both data controllers and data processors.

Member State supervisory authorities have already brought a number of enforcement actions since the GDPR went into effect. The UK's Information Commissioner's Office ("ICO"), for example, brought an enforcement action against a Canadian company for violating Articles 5, 6 and 14 of the GDPR, which also concurrently demonstrates the GDPR's extraterritorial reach. Moreover, high-profile GDPR actions and, in some cases, significant financial penalties, have been levied against other major companies, some of which are based outside of Europe. In addition, supervisory authorities have reported that the number of complaints filed by data subjects and the number of notifications of personal data breaches have increased substantially, in some cases increasing by as much as 10 times that of pre-GDPR times. Accordingly, the number of enforcement actions is likely to increase substantially in 2019.

We also expect to see more and expanded guidance from regulatory bodies on GDPR compliance issues in 2019. Various supervisory authorities, including the European Data Protection Board ("EDPB"), have already released guidance on the GDPR. These guidance documents build upon that which has already been released by the Article 29 Working Party. Notably, the EDPB has released guidelines on the territorial scope of the GDPR and on the derogations of Article 49.

CCPA. If 2018 saw the final push to prepare for GDPR compliance, then 2019 will likely see a similar effort by relevant companies to develop compliance mechanisms for the new California Consumer Privacy Act ("CCPA"). Set to take effect in 2020, (with the law becoming operative on January 1, 2020 and enforcement actions delayed until July 1, 2020), this law is the most sweeping general privacy statute in the United States. It protects an expansive set of consumer information and applies to companies across economic sectors. The law also constitutes a departure from prior US privacy regulation in its provision of

new protections and rights to consumers with regard to their personal information. In some respects, the CCPA bears resemblance to the GDPR, and, accordingly, a company may be able to leverage capabilities developed in response to the GDPR in its CCPA compliance efforts, particularly regarding disclosure requirements and subject access rights. However, these legal frameworks are not identical, and in 2019 companies will need to determine what new or modified mechanisms CCPA will require. Further complicating this task, many expect the CCPA to be amended before it takes effect in 2020, although the nature of any such amendments remains unclear, and several significant provisions of the CCPA are subject to implementing regulations to be issued by the California Attorney General on an uncertain timeline. Only the Attorney General can enforce the CCPA, with one notable exception: the CCPA grants consumers a private right of action for the unlawful exfiltration or disclosure of limited categories of personal information.

Brazilian General Data Protection Law. Another law inspired by the GDPR is Brazil's new General Data Protection Law (Lei Geral de Proteção de Dados, or "LGPD"). The LGPD was signed into law in August 2018 and amended in December 2018 by an executive order. Among the changes made by the executive order are that the LGPD will become effective in August 2020, six months after the initially scheduled date of February 2020. The LGPD is very similar to the GDPR, such as in terms of material scope, definitions, principles, security requirements and data breach notification requirements. The law also has extraterritorial applicability, similar to the GDPR. There are, however, some differences. For example, the LGPD contains some additional, more specific bases for processing that are not covered by the GDPR, such as for the protection of health in a procedure carried out by health professionals and the protection of credit. The potential fines are also lower than those under the GDPR— violations can result in fines of up to the higher of 2% of the company's gross revenue in Brazil the previous year or R$50 million. Still, companies subject to the LGPD will likely undertake substantial compliance work in 2019.

Other Jurisdictions. Other jurisdictions also are considering data protection laws that are similar to the GDPR. In the United States, for example, legislators in certain other states, such as New Mexico, have proposed laws similar to the CCPA. In addition, other countries, such as India, are considering laws inspired by the GDPR. Discussion and debate around the prospect of expanded and new legal regimes for data

privacy with global applicability and consequences will likely be prominent in 2019.

Focus on Data Privacy and Cybersecurity Policy

Policymakers at the state and federal level are poised to focus intensely on data privacy and cybersecurity issues in 2019. Debates over data privacy are likely to consider the respective roles of state and federal governments in regulating this important issue. Cybersecurity policy, meanwhile, is likely to have a particular focus on addressing and responding to threats posed by foreign actors. Policy decisions in both areas are likely to have significant consequences for the private sector, so businesses may benefit substantially from monitoring and engaging in these important policy debates.

DATA PRIVACY

The respective roles of state and federal governments in data privacy policy will be a key issue in 2019.

As discussed above, the California Consumer Privacy Act creates new rights for consumers regarding the transparency, collection, usage, sharing, deletion and sale of personal information. Lawmakers in other states already are pursuing similar legislation, dramatically increasing the chances that companies doing business in the United States will soon have to manage a patchwork of comprehensive privacy regimes across individual states.

Many corporations and industry associations will likely mobilize to push for a single federal data breach notification standard as part of such a law, as reflected in a number of recent private sector recommendations on the topic. Businesses will benefit from monitoring developments in this space as proposed legislation could have significant financial and operational consequences. For example, one bill proposed at the end of 2018 would have imposed duties of care, loyalty and confidentiality on online service providers that are engaged in interstate commerce over the Internet and collect identifying data about end users. While the timeframe for passing privacy legislation into law may stretch into the coming years and success is never certain, stakeholder commitment to the effort is real, and we expect that it will take up a good deal of legislators' attention in the coming year.

Congress also is likely to focus oversight activities on data privacy in 2019. Data privacy was covered in a number of prominent oversight hearings in 2018 that largely reacted to high-profile events and centered mostly on social media companies. Congressional oversight is

expected to increase significantly in 2019, especially with Democratic leadership of the House of Representatives. For example, the incoming leadership of the House Energy and Commerce Committee has indicated that privacy oversight will be high on its agenda in 2019. We expect that this oversight will relate to companies' use of consumer information and on the choices and knowledge consumers have about the use of their data. We also anticipate that oversight hearings will focus on the issues receiving the most public attention, which include data breaches, the security of user data and the use of sensitive personal information (such as biometric and geolocation data).

The Trump administration also is likely to focus on data privacy policy in 2019. In November 2018, the National Telecommunications and Information Administration received public comments from over 200 organizations as it sought to develop the administration's approach to consumer privacy. In addition, the National Institute of Standards and Technology has begun its own process to develop a privacy framework based on its highly successful cybersecurity framework. Both of these processes should be active throughout 2019.

Finally, even as companies carefully track data privacy developments in the United States at the state and federal level, the issue continues to take on global salience as well. In June, the G20 summit meeting in Japan will focus on global data governance. Speaking at the World Economic Forum in January, Japanese Prime Minister Shinzo Abe argued for updating World Trade Organization rules to account for and facilitate the free and secure flow of data globally. His comments were echoed by other world leaders. Although these were initial discussions, and no single proposal or policy solution has appeared to gain prominence, multinational businesses would do well to follow the evolution of global perspectives on these topics and weigh opportunities to engage in the ongoing debate.

CYBERSECURITY

The challenges posed by cybercrime and cyber-espionage are likely be central to US cybersecurity policy in 2019, both domestically and in its foreign relations. Private sector entities may have opportunities to work with the federal government in addressing such pressing issues, and potentially stand to benefit from monitoring evolving developments in this area.

Trade Secret Theft. Companies should expect the current Administration to remain focused on the threat to American economic prosperity and national security posed by economic espionage in 2019. In

2015, China and the United States publicly committed to not engage in the cyber-enabled theft of intellectual property for commercial gain. Recent statements from senior administration officials and high-profile indictments brought by the Department of Justice indicate the view of some leading government officials that China has failed to adhere to that commitment. For example, the Department of Justice indicted two Chinese nationals associated with the Chinese Ministry of State Security of numerous hacking offensives associated with a global campaign to steal sensitive business information. Congress is also likely to consider legislative responses to trade secret theft and economic espionage. These actions suggest that 2019 is likely to see further disputes with China over cyber theft of trade secrets. Companies—especially those in industries that have previously been targeted by espionage campaigns— are likely to benefit from tracking developments in this space.

DHS Reorganization. On November 16, 2018, President Trump signed the Cybersecurity and Infrastructure Security Agency Act of 2018, thereby effectuating a significant reorganization of cybersecurity capabilities at DHS. This legislation established the Cybersecurity and Infrastructure Security Agency ("CISA") as the entity within DHS that is "responsible for protecting the Nation's critical infrastructure from physical and cyber threats." In this role, CISA manages significant public-private cybersecurity engagement and information sharing, including through the National Cybersecurity and Communications Integration Center. 2019 will likely see opportunities for companies to continue building relationships with DHS on cybersecurity issues, including through initiatives championed under its new organization.

White House Cyber Strategy. The Trump administration released its first expansive National Cyber Strategy in September 2018. Building on the Administration's first executive order addressing cybersecurity, this document identified key goals and related actions to "ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity." Many of the priority actions identified in this strategy have the potential to impact private sector entities and could be pursued by the government in 2019. For example, the strategy prioritizes "risk-reduction activities across seven key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation." Companies in these industries can expect increased cybersecurity engagement from government actors. Notably, the strategy eschewed a regulatory approach

and, instead, called for "promot[ing] open, industry-driven standards . . . and risk-based approaches to address cybersecurity challenges." Companies and trade associations thus stand to benefit from remaining focused on government activity related to the National Cyber Strategy. However, there are potential risks associated with some of the administration's cybersecurity policies, including with respect to offensive cyber operations. In conjunction with the release of this national strategic position, the Administration altered the rules governing such military operations and authorized certain unspecified additional cyber activities against America's adversaries. Some commentators have raised concerns that such activities could lead to retaliation by foreign nation-states. The private sector will want to watch these developments carefully, especially as 85% of the nation's critical infrastructure—a primary target for cyber attack by malicious actors—is owned and operated by private entities.

EU Cyber Strategy. 2018 ended with a political agreement reached by EU institutions on the Cybersecurity Act (the "Act"). The Act paves the way for EU cybersecurity certification schemes for ICT products (i.e., hardware and software elements of network and information systems); services (i.e., services involved in transmitting, storing, retrieving, or processing information via network and information systems); and processes (i.e., sets of activities performed to design, develop, deliver and maintain ICT products and services). Another EU legislation that will have an impact on many companies' activities in 2019 is the Directive on Security of Network and Information Systems (the "NIS Directive"). The NIS Directive imposes specific security and notification requirements on operators of essential services (in sectors such as health, transport, financial market infrastructure and banking, water supply and distribution) and for digital services providers. Many national laws implementing the NIS Directive will enter into force in the coming year. Hence, affected companies will benefit from following these cybersecurity developments both at the EU and national levels.

Conclusion

Cybersecurity and data privacy are likely to stand among the most significant issues that multinational businesses must address in 2019. Cyber incidents continue to become more complex and severe, requiring companies to continue to refine their response capabilities, and legal frameworks, regulatory expectations, litigation risk, and policymaking continue to evolve, constantly adding complexity for

companies. Businesses will benefit from continuing to refine their cyber risk management and data privacy compliance programs to address these evolving challenges in the coming year.

CYBERSECURITY & DATA PRIVACY

With our global platform and our experienced and practical team of cybersecurity and data privacy lawyers, our firm can serve clients across a full range of domestic, international and cross-border privacy issues.

The cybersecurity landscape is evolving more rapidly than ever before, and the threats to businesses' critical information and assets—as well as to their bottom lines—are only increasing. Breaches continue to grow in scale and sophistication, regulators are crowding the field with an expanding and shifting array of requirements and de facto standards, and litigation remains perilous. Now, more than ever, businesses must think strategically about the cyber threats they face—whether to consumer or employee information, intellectual property or product safety—and take practical steps to address the associated legal, business and reputational risks.

Mayer Brown brings a comprehensive and integrated approach to cybersecurity and data privacy challenges, offering our clients strategic thinking and practical legal advice. Our practice is composed of more than 50 lawyers worldwide from disciplines that include litigation, regulatory, corporate, government affairs and global trade, intellectual property, enforcement, employment, insurance and technology transactions. We leverage our broad and deep experience in these key disciplines to build tailored teams to address the specific issues that our clients face. This approach to our Cybersecurity & Data Privacy practice distinguishes us from other firms that rely on "one size fits all" privacy and security lawyers who attempt to cover the waterfront of these ever-increasing and complex issues.

The firm's global platform enables us to provide exceptional service to our clients across the globe. Mayer Brown and affiliated lawyers located throughout the Americas, Europe and Asia have deep knowledge and a practical understanding of the cybersecurity and data privacy statutes and regulations in their home countries and surrounding regions. This experience and global capability allows us to address a client's most complex international cybersecurity and data privacy issues, whether they require advice on creating an enterprise-wide privacy framework, counsel on international data transfers, or assistance in responding to a data breach in multiple jurisdictions. Together, our

lawyers help clients respond proactively to international developments, whether in Europe, Hong Kong, Brazil, or elsewhere around the globe. In addition, our practice maintains an extensive network of local counsel in countries where we do not have offices and with whom our lawyers liaise as needed.

PUBLICATIONS:

2018 Cybersecurity and Data Privacy: Navigating a Constantly Changing Landscape

Cybersecurity and Data Privacy: Navigating a Constantly Changing Landscape highlights developments and priorities for businesses on a range of key topics, from the compliance challenges posed by new regimes such as the EU General Data Protection Regulation and the New York's financial services regulations, to growing expectations for due diligence in mergers and acquisitions, to evolving threats that demand thorough response playbooks.

To request a copy of this guide, please visit: mayerbrown.com/Cybersecurity-and-Data-Privacy-Navigating-a-Constantly-Changing-Landscape-09-27-2018/

2017 Staying Ahead of the Curve: Cybersecurity and Data Privacy— Hot Topics for Global Businesses

Staying Ahead of the Curve: Cybersecurity and Data Privacy—Hot Topics for Global Businesses, highlights key developments and priorities in these critical fields, from the Internet of Things and the cloud to complying with China's new cybersecurity law and Europe's General Data Protection Regulation.

To request a copy of this guide, please visit: mayerbrown.com/staying-ahead-of-the-curve-cybersecurity-and-data-privacyhot-topics-for-global-businesses-09-28-2017

2016 Cybersecurity Regulation in the United States: Governing Frameworks and Emerging Trends

Cybersecurity Regulation in the United States: Governing Frameworks and Emerging Trends offers insights on the regulatory frameworks applicable across key sectors of the United States economy, as well as emerging regulatory trends across sectors.

To request a copy of this guide, please visit: mayerbrown.com/Cybersecurity-Regulation-in-the-United-States-Governing-Frameworks-and-Emerging-Trends-09-29-2016

2015 Preparing For and Responding To a Computer Security Incident: Making the First 72 Hours Count

Preparing For and Responding To a Computer Security Incident: Making the First 72 Hours Count offers insights on how to prepare for a computer security incident and how to implement a timely, effective response.

To request a copy of this guide, please visit: mayerbrown.com/preparing-for-and-responding-to-a-computer-security-incident-making-the-first-72-hours-count

Contributors

For more information about the topics raised in this 2019 Outlook, please contact any of the following contributing Cybersecurity & Data Privacy practice team lawyers. Learn more about our full team and practice here: mayerbrown.com/experience/cybersecurity-data-privacy

Rajesh De
Global Cybersecurity & Data Privacy Practice Leader
+1 202 263 3366
rde@mayerbrown.com

Matthew Bisanz
+1 202 263 3434
mbisanz@mayerbrown.com

Samantha C. Booth
+1 312 701 8327
sbooth@mayerbrown.com

Kendall C. Burman
+1 202 263 3210
kburman@mayerbrown.com

Marcus A. Christian
+1 202 263 3731
mchristian@mayerbrown.com

Diletta De Cicco
+32 2 551 5945
ddecicco@mayerbrown.com

Cristiane Manzueto
+55 21 2127 4235
cmanzueto@mayerbrown.com

Veronica R. Glick
+1 202 263 3389
vglick@mayerbrown.com

Charles-Albert Helleputte
+32 2 551 5982
chelleputte@mayerbrown.com

Sasha Keck
+1 202 263 3464
skeck@mayerbrown.com

Gabriela Kennedy
+852 2843 2380
gabriela.kennedy@mayerbrownjsm.com

Zaneta Kim
+1 650 331 2072
zkim@mayerbrown.com

Mickey Leibner
+1 202 263 3711
mleibner@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Ian McDonald
+44 20 3130 3856
imcdonald@mayerbrown.com

Christopher M. Mikson
+1 202 263 3157
cmikson@mayerbrown.com

John Nadolenco
+1 213 229 5173
jnadolenco@mayerbrown.com

Mark A. Prinsley
+44 20 3130 3900
mprinsley@mayerbrown.com

Linda L. Rhodes
+1 202 263 3382
lrhodes@mayerbrown.com

Lei Shen
+1 312 701 8852
lshen@mayerbrown.com

Benjamin Shoemaker
+1 202 263 3463
bshoemaker@mayerbrown.com

Joshua M. Silverstein
+1 202 263 3208
jsilverstein@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

Emily K. Strunk
+1 202 263 3404
estrunk@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

Matthew A. Waring
+1 202 263 3273
mwaring@mayerbrown.com

Jonathan Weinberg
+1 202 263 3442
jweinberg@mayerbrown.com

Oliver Yaros
+44 20 3130 3698
oyaros@mayerbrown.com

Lisa V. Zivkovic
+1 212 506 2482
lzivkovic@mayerbrown.com

KEEPING IT PRIVATE: GDPR AND DEVELOPMENTS IN DATA PRIVACY IN 2018

January 14, 2019

By Larry Hamilton, Charles-Albert Helleputte, Sanjiv Tata, Oliver Yaros, Kendall C. Burman, Diletta De Cicco and Evan M. Wooten[1]

---

1. Larry Hamilton leads Mayer Brown's US insurance regulatory practice within the Insurance Industry group. He advises insurance companies, insurance agencies and investment companies on a broad range of regulatory matters, including those associated with formation, licensing, portfolio investments, reinsurance, e-commerce, cybersecurity and outsourcing. He is also a member of Mayer Brown's Cybersecurity & Data Privacy practice. Charles-Albert Helleputte is a transactional and cyber security and data privacy lawyer. In the transactional context, he focuses his practice on domestic aspects of cross-border transactions, acquisitions, disposals, restructurings, financing and refinancing. Charles heads the cyber security and data privacy team in Brussels. Sanjiv Tata is an associate in Mayer Brown's New York office and a member of the Corporate & Securities practice, specializing in insurance regulatory work. Sanjiv advises insurance companies, insurance intermediaries and investment companies with respect to a broad range of insurance regulatory and corporate matters, including formation and licensing of insurance companies, mergers and acquisitions of insurance companies, reinsurance transactions, and enforcement, corporate governance, cybersecurity, enterprise risk and general compliance matters. Oliver Yaros is a partner in the Intellectual Property & IT Group as well as the Technology Transactions and Cybersecurity & Data Privacy Practices of the London office of Mayer Brown. He advises clients on technology and outsourcing transactions with a particular focus on fintech and digital transformation projects, as well as clients operating within a broad range of sectors on data protection matters and cybersecurity incidents, intellectual property transactions and related issues. Kendall Burman is a Cybersecurity & Data Privacy counsel in Mayer Brown's Washington DC office. Kendall advises a broad range of clients, including financial services and technology companies, on legal, regulatory, and policy issues involving emerging technologies, security, privacy, and the flow of information across borders. Diletta is an associate in the Brussels office. Her practice focuses on privacy and cyber security. Diletta advises clients regarding a wide range of global data privacy and security issues. She assists organizations in complying with EU and national privacy laws, including developing global data transfers mechanisms, privacy statements, data breach notification policies and procedures, etc. Diletta regularly publishes articles on those matters and is a speaker on such topics. Evan Wooten is an experienced civil litigator, focusing on privacy, consumer class action defense and actions by public officials and public enforcement bodies. Evan also assists clients in crafting contracts, policies, and terms of use to minimize litigation and government investigations. Evan is a member of Mayer Brown's consumer class action and commercial law groups and co-chairs the editorial team for the Firm's privacy and security newsletter and publications.

By any measure, 2018 was a major year for data privacy regulation. The most significant regulatory development in this area was the European Union's General Data Privacy Regulation ("**GDPR**"), which went into effect on May 25, 2018 and establishes what is probably the most rigorous data protection regime currently in existence. As adopted, GDPR includes numerous restrictions on the use of individual personal data, coupled with an expansive extraterritorial reach that makes compliance with its provisions a concern for many business who maintain even relatively minor connections with the European Union. Also in 2018, the State of California enacted the California Consumer Privacy Act ("**CCPA**"), which establishes a data protection regime that is in many ways inspired by GDPR and will come into effect on January 1, 2020.

GDPR and the heightened restrictions it establishes regarding the use of personal information will have a major effect on insurance industry participants that are subject to GDPR and to regulatory initiatives in other jurisdictions, such as California, that choose to adopt a similar framework. The collection and use of personal information is a core business practice of the insurance industry worldwide. Personal information is obtained by insurance companies, agents, brokers and other service providers in order to design, underwrite and distribute insurance products and services to consumers. Consequently, a data protection regime that could restrict such entities in accessing and processing personal information would require significant reevaluation of their foundational operational practices.

The General Data Privacy Regulation

GDPR is the result of a multi-stage negotiation process among the members of the European Union, originally proposed by the European Commission to replace the 1995 European Directive (95/46/EC) (the "**Directive**"), which set out the previously existing data protection regime for the European Union. Adopted by the European Parliament and the Council of the European Union on April 14, 2016, GDPR became enforceable on May 25, 2018. As a regulation (as opposed to a directive) it is directly binding and applicable in all Member States of the European Union.[2]

2. As of July 20, 2018, GDPR was also adopted by the three of the four nations in the European Free Trade Association – Iceland, Lichtenstein and Norway.

GDPR defines personal data as "information relating to an identified or identifiable natural person,"[3] and establishes a number of protections for and restrictions on use and transfer of such personal data. Crucially, GDPR sets a very low bar for what is considered "identifiable": if a natural person can be identified using "all means reasonably likely to be used,"[4] the information would be considered "personal data." Accordingly, data may be considered personal data even if the entity holding such data cannot itself identify the natural person to whom such data pertains. Indeed, the name of a natural person would not be required to establish that information is "personal data" – any identifier, including an identification number, location data, online identifier or other similar factor may be considered an identifying factor for a natural person.

While the GDPR includes many requirements, most relevant to insurers may be the significantly enhanced rights provided to individuals, and these enhanced rights are coupled with specific provisions that make it easier for such individuals to claim damages for compensation for violations of such rights. These rights include, with exceptions: (i) a right to access personal data in a concise, transparent and easily accessible form; (ii) a right in certain circumstance to have personal information erased ; (iii) a right to receive or have transmitted to another controlling entity all personal data concerning them in a structured, commonly used and machine-readable format; (iv) a right to object to the processing of personal data; and (v) a right not to be subject to automated decision making processes, including profiling.

As a practical matter, the extremely expansive definition of "personal data" means that organizations that must comply with GDPR will need to institute compliance practices across a far wider range of data processing and utilization practices than ever before. Further, even if an organization is not established within the European Union, it can still be subject to GDPR if it processes the personal data of individuals who are in the European Union where the processing activities are related "to the offering of goods or services"[5] to such individuals in the European Union or "the monitoring of their behavior"[6] to the extent that their behavior takes place within the European Union.

---

3. Art. 4 of GDPR.
4. Recital 26 of GDPR.
5. Art. 3(2)(a) of GDPR.
6. Art. 3(2)(b) of GDPR.

In order to comply with GDPR, organizations need to be in a position to affirmatively demonstrate to supervisory authorities and data subjects that they have affirmatively complied with the relevant provisions of the regulation. GDPR particularly sets out enhanced governance obligations, including requirements to: (i) keep a detailed record of processing operations; (ii) provide a fair processing notice to individuals whom personal data is being processed about that explains the purposes and legal basis of the processing as well as other information; (iii) perform data protection impact assessments for high risk processing; (iv) designate a data protection officer to advise on compliance with GDPR and generally monitor data protection efforts; (v) maintain a comprehensive record of data breaches, including notifying individuals where necessary; (vi) impose specific contractual requirements on third parties that personal data is shared with; and (vii) implement "data protection by design and by default."[7]

The California Consumer Privacy Act and the Consequences of GDPR in the United States

While its expansive territorial scope may make compliance with GDPR a top priority for large multinational holding companies (including those based in the United States), such companies will now need to consider privacy legislation adopted in the United States as well.

On June 28, 2018, the CCPA was enacted in California, and comparisons were immediately drawn to the GDPR. For purposes of the CCPA, "personal information" is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,"[8] a definition that has a similar broad scope to the definition utilized by GDPR.

The CCPA, like GDPR, imposes a number of restrictions on organizations beyond the physical borders of California, including on any organizations that control personal data and do business in

7. With respect to this last point, Article 25 of GDPR introduces the dual concepts of "data protection by design and by default." "Data protection by design" requires organizations to take into account the risks that could be presented to protecting an individual's personal data during the process of designing and implementing a new process, product or service. "Data protection by default" requires organizations to put in place mechanisms to ensure that, by default, only personal data that is strictly necessary for specific purpose is processed.
8. CAL.CIV.CODE § 1798.140.

California, albeit only subjecting those organizations to the extent that they process data of California residents. However, unlike GDPR, the CCPA has not set out any principles regarding the lawful processing of personal data – though given how recently the CCPA was passed and its effective date of January 1, 2020, there is a significant likelihood that California regulatory authorities, including the Attorney General, may issue guidance on this point. Indeed, the CCPA requires the Attorney General to issue regulations implementing certain of its provisions (for example, instructing how businesses can "reasonably verify" consumer requests) and authorizes the adoption of additional regulations as necessary to further the CCPA's purposes.

Similarly, the CCPA grants consumers who are California residents a number of rights, some of which are broadly analogous to the rights established by GDPR, including (with certain exceptions): (i) a right for consumers to receive affirmative disclosures from organizations covered by the CCPA of such organizations' sale, collection or disclosure of such individuals' personal information, and the requirement that such organizations respond to requests for information from such individuals; (ii) a right for consumers to access specific pieces of information collected about them by an organization; (iii) a right for consumers to request the deletion of their personal information from organizations that hold such information; (iv) a right for consumers to opt-out of the sale of personal information to third parties; and (v) a right of consumers not to be subject to discrimination for exercising their rights under the CCPA. The Attorney General may sue to enforce these rights, although private citizens may only sue to redress the unlawful exfiltration or disclosure of very limited categories of personal information (name, social security number, driver's license number and certain financial, medical and health insurance information).

In addition, a number of states have updated their data breach notification laws in the months following the effective date of GDPR, including Alabama, Arizona, Louisiana, Oregon and South Dakota. This would seem to indicate the growing importance of data privacy concerns to governmental authorities throughout the United States.

Likely Effects of GDPR in 2019 and Beyond

There is a significant likelihood that GDPR, with its increased protections for consumers, could reset the standard for how businesses, including insurance industry participants, handle personal data. Further, if protections of the type established by GDPR and the CCPA are adopted more widely, it is likely that individuals will become more

aware of the advantages afforded to them by businesses that are compliant with those protections and may choose (to the extent feasible) to provide their data to those businesses rather than to businesses that are not obligated to provide GDPR-style protections. Another potential consequence is that standard contracts customarily used throughout industries would need to be revisited with an eye towards compliance with an enhanced data privacy regime, including reexamination of commercial terms given the increased costs of compliance with and higher risks of non-compliance under such a regime.

Ultimately, laws such as GDPR represent a paradigm shift for data-centric industries, like insurance, which are anchored in the use of personal information. While many insurance industry participants have begun to adjust for the increased restrictions of GDPR, these regimes present more than cosmetic legal and compliance challenges, but require companies to overhaul their thinking on the way that they collect, process, store, share and discard personal data. If regimes similar to GDPR and the CCPA are adopted more widely, basic services provided by insurance companies, agents, brokers and other service providers, down to the issuance of policies and processing of claims, will have to be reevaluated in the light of the enhanced protections for personal data and increased consent rights for individuals. Although it remains to be seen whether and to what extent lawmakers and regulators in the United States and other non-EU countries will adopt GDPR-like laws and regulations, companies would do well to remain attuned to and anticipate the changing regulatory environment that is increasingly sensitive to safeguarding the privacy of personal data. It will also be important for industry representatives to engage with their legislators and regulators in order to have a voice in shaping future legislative and regulatory initiatives.

TOP TIPS: PREPARING TECHNOLOGY ARRANGEMENTS FOR BREXIT

January 2019

Mayer Brown Legal Update

The ultimate form of the UK's exit from the European Union remains a hotly debated topic. Unless some form of extension of the period of notice served by the UK is agreed in the next few weeks or the notice is withdrawn, the UK will leave the European Union on 29 March 2019. In January, the UK Parliament will be faced with a choice of accepting the Draft Withdrawal Agreement produced by the negotiating teams of the UK and the EU as at November 2018 or leaving the EU without a finalised transition agreement, the so-called "No Deal" scenario.

The Draft Withdrawal Agreement covers a number of issues of direct relevance to technology arrangements. The purpose of this alert is to highlight some key risks of either the No Deal scenario or a deal on the terms of the Draft Withdrawal Agreement which relate specifically to technology arrangements and to steps to mitigate these risks.

1. Personal data issues

The General Data Protection Regulation ("GDPR") implemented in 2018 updated the law relating to the treatment of personal data within the European Union. The UK also passed UK specific domestic legislation–The Data Protection Act 2108–which will ensure that post departure from the European Union the UK will treat personal data in exactly the same way as it is treated today under the GDPR; so Brexit is not going to mean a further wholesale revision of data protection policies and procedures for UK businesses.

UK businesses will nevertheless need to consider the basis upon which personal data can be transferred internationally. The UK government has indicated that it will (continue to) treat the remaining EU countries as having adequate data protection regimes, so no additional steps will need to be taken to transfer personal data to the remaining EU countries.

What is currently less clear is whether transfers of personal data from the remaining EU countries to the UK will be permitted on the basis that the UK is deemed to (continue to) have an adequate data protection regime. In the absence of an adequency finding in relation to UK data protection laws an alternative basis will have to be relied upon

to enable personal data to be transferred from the remaining EU countries to the UK.

The Draft Withdrawal Agreement provides that the UK will continue to apply Union law in the United Kingdom in respect of processing of personal data of data subjects outside the United Kingdom provided that personal data is covered by the Draft Withdrawal Agreement- in broad terms, the personal data relates to EU residents. This should make it likely that the UK will be seen by the other EU countries to have an adequate regime post Brexit if the Draft Withdrawal Agreement comes into effect. If the UK leaves on a No Deal basis then it is far from clear that the remaining EU countries will see the UK as having an adequate data protection regime.

Businesses transferring personal data between the remaining EU countries and the UK should be considering alternative bases for transferring personal data from the remaining EU countries to the UK as a result of Brexit. The simplest solution for most businesses is likely to be putting in place the EU approved Standard Contractual Clauses.

Businesses exporting personal data from the UK to third countries will also have to ensure that they comply with the UK specific rules on export of personal data from the UK to third countries. A particular point to look out for is whether all the countries which the EU has accepted as having an adequate data protection regime will be regarded by the UK as also having an adequate data protection regime. The risk of the UK taking a different position to the EU in relation to existing adequacy decisions seems extremely low.

2. Protection of Databases

Most Intellectual Property rights exist independently of the treaties between Members of the EU and the existence of these rights will not be affected by the UK's departure from the EU. There is, however, a specific EU right that protects databases – the so-called Sui Generis right which was created by the EU Database Directive in 1996, which may be significant for some technology arrangements.

When the UK leaves the EU, the Directive will cease to apply to the UK. Under the Draft Withdrawal Agreement, a database will continue to be protected where it is created by UK nationals, natural persons with habitual residence in the UK or businesses established in the UK. In the No Deal scenario, the ironic position will be that EU nationals, residents and businesses in the UK will acquire the Sui Generis right when they develop databases in the UK but UK nationals, residents and businesses will not. The UK Intellectual Property Office

is alive to this concern and will push for reform of UK law to give UK nationals, residents and businesses equal protection under a domestic Sui Generis right (which, in fact, existed in the UK prior to the EU Database Directive in any event). Without agreement with the remaining EU countries the UK domestic right will not give rights which extend to the remaining EU countries.

It is unclear just how significant the Sui Generis right is in practice, but UK domestic businesses can minimise the risk of losing protection for databases developed in the UK by involving developers with an EU connection. Also, the database would be protected internationally through the copyright system if sufficient creativity can be established for the database to be protected as a copyright work. Careful records should be maintained showing the development process and it is possible that copyright protection may be available.

3. Free movement of goods

Many businesses have been concerned about fractured supply chains if the UK leaves the EU in a No Deal scenario. Similar concerns will apply for technology arrangements where continued access to hardware and consumables will be required. In the Draft Withdrawal Agreement scenario goods first lawfully put on the market in the EU or in the UK prior to the end of the transition period can circulate between the two markets before they reach the end user. In the Draft Withdrawal Agreement scenario, there should therefore be minimal disruption to international shipments between the remaining countries in the EU and the UK for a period of time. To prepare for the No Deal scenario businesses should, however, be revisiting their supply chains and inventory to ensure that the impact of delays in customs processes etc. are minimised.

4. Free movement of people

In order to assess fully the potential HR implications of Brexit, whether under the Draft Withdrawal Agreement or in a No Deal scenario, businesses should carry out a 'people audit'. This should map out the locations of the direct workforce and, for outsourced arrangements, those of its third party suppliers. Specifically, how many UK nationals are working in the EU and how many EU nationals are working in the UK. This will highlight the potential implications of a change in immigration requirements as a result of Brexit.

The UK Government has made clear that, regardless of the outcome of the EU negotiations, it will proceed with its settlement scheme which will allow EU nationals to apply for settled status, provided they have arrived in the UK by the end of 2020. The government has indicated that the scheme for EU nationals to apply for settled status will open fully by March 2019. Businesses should consider helping those who qualify for the scheme to take advantage of it, particularly if they are in key roles. After 2020, the UK is likely to have a new post-Brexit immigration system. The current Government proposal is for a single, unified system which offers no preference for EU workers ahead of non-EU workers, but provides priority instead to highly-skilled workers.

In relation to UK nationals based in the EU, some EU governments—for example the Netherlands— have made welcoming noises, promising measures to allow such individuals to remain there after March 2019 in the event of a No Deal scenario. Using the results of the people audit, businesses should focus on those EU countries that are most relevant to its workforce and monitor developments of any such legislation. They may also consider whether UK nationals working in the EU are able to apply for a right to remain there based on residency, marriage or ancestry.

5. Review technology supply agreements

For all material technology arrangements contractual frameworks should be reviewed in the context of Brexit. Pan-European arrangements should be an area of particular focus.

Key contractual provisions to review will include:

- Territorial scope of licences
- Location of Personal Data
- Rights in Databases
- Currency/inflation indices
- Compliance with laws obligations
- TUPE/ARD on termination

For further information, please contact:

Mark Prinsley
Partner, London
E: mprinsley@mayerbrown.com
T: +44 20 3130 3900

Christopher Fisher
Partner, London
E: cfisher@mayerbrown.com
T: +44 20 3130 3724

Andrew Stewart
Partner, London
E: astewart@mayerbrown.com
T: +44 20 3130 3929

Oliver Yaros
Partner, London
E: oyaros@mayerbrown.com
T: +44 20 3130 3698

Daniel Gallagher
Senior Associate, London
E: dgallagher@mayerbrown.com
T: +44 20 3130 3537

Valerie Vanryckeghem
Advocaat (Brussels), London
E: vvanryckeghem@mayerbrown.com
T: +44 20 3130 3074

Ryota Nishikawa
Associate, London
E: rnishikawa@mayerbrown.com
T: +44 20 3130 3189

DOJ RELEASES UPDATED CYBER INCIDENT RESPONSE GUIDANCE FOR PRIVATE SECTOR ENTITIES

1 November 2018

Mayer Brown Legal Update

On September 27, 2018, the Computer Crime and Intellectual Property Section ("CCIPS") of the Criminal Division in the US Department of Justice ("DOJ") released a revised version of its *Best Practices for Victim Response and Reporting of Cyber Incidents*. Although primarily targeted to "smaller organizations and their legal counsel," this guidance on preparing for and responding to cyber incidents may be helpful to private sector entities of all sizes. It expands on guidance issued by CCIPS in April 2015 and is intended to "help organizations prepare a cyber incident response plan and, more generally, to better equip themselves to respond effectively and lawfully to a cyber incident." The updated guidance addresses new topics, including the impact of the Cybersecurity Information Sharing Act of 2015 ("CISA") and working with external support such as cyber incident response firms.

Organized according to the chronology of cyber incident preparation, response and recovery, the revised guidance provides advice under four overarching headings:

1. Steps to Take Before a Cyber Intrusion or Attack Occurs
2. Responding to a Cyber Incident: Executing Your Incident Response Plan
3. What Not to Do Following a Cyber Incident
4. What to Do After a Cyber Incident Appears to Be Resolved

Below we outline the revised guidance and discuss the new material that the DOJ has added to incorporate information learned from companies that have responded to cyber incidents.

Steps to Take Before a Cyber Intrusion or Attack Occurs

The first section of the DOJ's guidance focuses on steps that companies should take to prepare for and mitigate the damage associated with a cyber incident. These steps are as follows:

A. Educate Senior Management About the Threat

B. Identify Your "Crown Jewels"

C. Have an Actionable Plan in Place … Now!

D. Engage with Law Enforcement Before an Incident

E. Have Appropriate Workplace Policies in Place

F. Institute Basic Cybersecurity Procedures

G. Procure Appropriate Cybersecurity Technology and Services Before an Incident Occurs

H. Have Appropriate Authorization in Place to Permit Network Monitoring

I. Ensure Your Legal Counsel Is Familiar with Technology and Cyber Incident Management

J. Establish Relationships with Private and Public Cyber Information-Sharing and Analysis Organizations

Many of these topics—such as the identification of an organization's informational "crown jewels," implementation of incident response plans, and engagement with law enforcement—were addressed by the April 2015 guidance. However, the updated guidance builds on these and other discussions significantly. For example, the 2015 guidance discussed the value of having "ready access to the technology and services that [a company] will need to respond to a cyber incident"; the updated guidance expands on this by highlighting specific issues and benefits associated with retaining cybersecurity incident response firms and cloud storage services. In addition, building on the recommendation in the 2015 guidance to implement real-time network monitoring in a lawful manner, the updated guidance offers more detail on the applicable legal framework, including the role of CISA in "provid[ing] private entities with broad authority to conduct cybersecurity monitoring of their own networks, or a third party's networks with appropriate consent." (See our Legal Update.) Relatedly, the updated guidance provides an expanded discussion of information sharing, acknowledging historic private sector concerns with such sharing and highlighting how CISA and other federal guidance address some of those concerns, including with respect to federal antitrust laws.

The DOJ has also added completely new sections. For example, the updated guidance addresses the increasingly prevalent topic of oversight of cybersecurity programs by senior management and boards of directors, stating that "an organization's senior management, board of trustees, and any other governing body responsible for making resource decisions and setting priorities should be aware of how cyber threats can disrupt an organization, compromise its products, impair

customer confidence and relations, and otherwise cause costly damage." The guidance recommends "regular briefings" and "[c]yber incident preparedness exercises" as possible strategies for satisfying this evolving governance expectation.

The guidance also devotes new sections to actions that can help prevent cyber intrusions. In a section on "[a]ppropriate [w]orkplace [p]olicies," the DOJ recommends that organizations "adopt internal policies and rules that will help ensure that [] personnel are familiar with the incident response plan" and establish employee policies to mitigate insider threats, such as by ensuring that credentials are quickly disabled for terminated employees. In a separate, new section on instituting basic cyber hygiene, the DOJ encourages organizations to "adopt and maintain commonsense cybersecurity practices." Examples of such practices include the use of a "reasonable patch management program," "access controls and network segmentation" and "password management programs." This advice expands the focus of the DOJ's guidance from incident response to include general prescriptions for cybersecurity preparedness and the implementation of an information security program.

Responding to a Cyber Incident: Executing Your Incident Response Plan

The next section of the DOJ's guidance provides a step-by-step approach to responding to a cyber incident. The recommended steps are:

1. Make an Initial Assessment
2. Implement Measures to Minimize Continuing Damage
3. Record and Collect Information
4. Notify

The revised guidance takes these overarching topics from the 2015 guidance and expands the discussion, adding subsections to address additional concerns. For example, the updated guidance supplements the first step's focus on data collection activities with new advice for collaborating with incident response firms. The guidance advises companies to choose a provider that can employ "forensically sound methods of evidence collection" and data preservation techniques to ensure that information remains usable as evidence in a potential prosecution related to an attack. The guidance also discusses companies' legal concerns about disclosing forensic reports drafted by such firms following an incident. Specifically, the guidance describes the value of sharing

such documents with law enforcement and suggests strategies for mitigating associated risks, such as by sharing a summary, creating an excerpted version or providing only technical data.

The updated guidance also includes an expanded discussion of incident notification. It notes that "[a] victim of a cyber incident can receive assistance from federal agencies that are poised to investigate the incident, help mitigate its consequences, and help prevent future incidents." In this vein, the guidance now includes a new section that highlights the "[b]enefits of [c]ontacting [l]aw [e]nforcement." Building on the prior guidance, the DOJ describes incident response services provided by the FBI's Cyber Action Teams. Notably, the DOJ also discusses how CISA has "made cooperating with law enforcement simpler by addressing common concerns about legal impediments to sharing information with the government." Specifically, "CISA authorizes nonfederal entities to voluntarily share 'cyber threat indicators' and 'defensive measures' with law enforcement for a cybersecurity purpose, notwithstanding any other provision of law."

What Not to Do Following a Cyber Incident

In this section, the revised guidance identifies certain actions that companies should not take in their response to a cyber incident. For example, the DOJ advises private sector entities against using a compromised system to communicate about an ongoing investigation or containment effort. The guidance also encourages companies not to "hack" into or damage third-party networks in responding to an incident. In 2015, the DOJ stated that attempting to gain unauthorized access to third-party networks "is likely illegal, under U.S. and some foreign laws, and could result in civil and/or criminal liability." The revised guidance maintains this position, stating that such activity "may violate federal law and possibly also the laws of many states and foreign countries, if the accessed computer is located abroad. A violation of those laws could result in civil and criminal liability." The updated guidance provides additional information about the potential unintended consequences of "hacking back," such as "targeting an unwitting, innocent victim whose system is being exploited by the perpetrator" and violating third-party privacy rights. It also notes that such activity could interfere with ongoing law enforcement investigations, such as by leading a perpetrator to "change tactics or modify operations if he or she detects a hack back attempt."

What to Do After a Cyber Incident Appears to Be Resolved

Finally, the updated guidance contains a new section addressing post-incident activities, including monitoring for "new signs of re-infection or compromise" by intruders. In addition, the DOJ advises companies to take steps to prevent future incidents, such as by "addressing shortcomings in [] security practices, acquiring resources to better secure [] systems, and fortifying relationships with law enforcement and other key response organizations."

Conclusion

This guidance represents an evolution in the DOJ's approach to private sector engagement on cybersecurity challenges. It was released in tandem with a cybersecurity roundtable discussion that "included many of the nation's leading private-sector practitioners in the field of data breach response and representatives from premier cybersecurity and incident response firms in the country."[1] Since the establishment of the Cybersecurity Unit within CCIPS and the release of the first version of the DOJ's cyber incident response guidance, "the Department [has] continue[d] to exchange ideas with and look to the private sector's expertise and insight about how to improve cooperation between law enforcement agencies and data breach victims." The DOJ views its updated guidance as part of this ongoing effort and as a resource for private sector entities to use in preparing for and responding to cyber incidents, especially when evaluating the risks and benefits of law enforcement engagement.

1. Press Release, DOJ, Justice Department Hosts Cybersecurity Industry Roundtable (Sept. 28, 2018), https://www.justice.gov/opa/pr/justice-department-hosts-cybersecurity-industry-roundtable.

CALIFORNIA ENACTS FIRST STATE LAW TARGETING IOT CYBERSECURITY

16 October 2018

Mayer Brown Legal Update

On September 28, California Governor Jerry Brown signed a first-of-its kind law to regulate the security of connected devices that make up the "Internet of Things" ("IOT")—connected fitness trackers, smart appliances, home alarm systems and much more.

The rapid adoption of these connected devices has led to an increase in security risk and a corresponding rise in government interest in IoT security. US federal agencies such as the Department of Homeland Security and the Department of Commerce have provided guidance on how to manage the security of these devices, and the Federal Trade Commission ("FTC") has asserted its authority to bring enforcement actions for "unreasonable" IOT cybersecurity practices.

On the other hand, state governments have not engaged on IOT cybersecurity, but that now has changed. The California law creates new regulatory concerns for manufacturers of connected devices sold in the state. As a result, businesses that manufacture connected devices will benefit from monitoring how the law is implemented and whether other states follow suit with their own laws to regulate connected device cybersecurity.

The California law, which goes into effect on January 1, 2020, sets requirements for manufacturers of a "connected device." This term is broadly defined to include "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address." However, the bill includes a number of exceptions to this scope. In particular:

- The statute does not apply to "any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority."
- Likewise, the statute does not apply to persons subject to the Health Insurance Portability and Accountability Act with respect to any activity regulated by those acts.

The sweep of these exceptions will be of great interest to manufacturers in a range of sectors. Manufacturers of connected cars and medical devices, for example, are likely to view the guidance issued by the National Highway Traffic Safety Administration and the Food and Drug

Administration, respectively, as removing their products from the scope of the California statute (even assuming that this statute otherwise can or does apply). Moreover, manufacturers of other consumer products may well view the FTC's guidance on IOT security and data security more broadly as excepting their products from the statute's sweep. Finally, while the statute is clearly aimed at the new wave of connected devices used by consumers, it remains to be seen whether efforts will be made to apply the law to products that are not directly marketed to consumers or to apply its requirements to more conventional information technology products that are not normally considered part of the IOT (e.g. laptops, tablets).

For devices that are within the state law's scope, manufacturers must ensure that these connected devices have "reasonable" security features that are:

- Appropriate to the device's nature and function;
- Appropriate to the information the device collects, contains or transmits; and
- Designed to protect the device and its information from unauthorized access, destruction, use, modification or disclosure.

The statute takes particular aim at generic, hard-coded device passwords. For devices that can be authenticated outside a local area network, it specifies that unique preprogrammed passwords or a requirement that a user generate a new password before initially using the device are deemed "reasonable" security features. Beyond this particular point, however, the law does not provide more detail on how a manufacturer can determine whether the security measures it adopts meet this reasonableness.

Importantly, the new law also specifies that it does not create a private right of action. Whether that is the final word on civil litigation remains to be seen, however. Plaintiffs already have brought claims under the California Unfair Competition Law ("UCL") for alleged security flaws in connected devices, for example. While the California Supreme Court has previously made clear its unwillingness to allow plaintiffs to use the UCL to do an end run around more specific statutory schemes that limit liability, plaintiffs nonetheless may seek to rely on the standards stated in California's new IOT law in common law or UCL claims.

Moreover, the law does provide the California attorney general, city, county or district attorneys with enforcement authority. How this law is interpreted and enforced by this broad group of government agencies remains to be seen. The statute ultimately may prove, for example, to reinforce the requirements already applicable to connected device

manufacturers subject to the jurisdiction of the FTC or sector-specific regulators. However, the possibility of divergent legal requirements—and even the creation of a patchwork of similar, but not identical, laws in other states—makes this statute a very significant development in the regulation of IOT cybersecurity. Manufacturers of connected devices consequently are likely to be well-served by closely monitoring further developments in this area.

5 CONSIDERATIONS FOR GENERAL COUNSELS REGARDING THE NEW YORK CYBERSECURITY REGULATIONS

21 February 2019

Mayer Brown Legal Update

The cybersecurity regulation ("CyberRegs") adopted by the New York State Department of Financial Services ("NYDFS") is almost two years old and will be fully in effect by March 2019.[1] The CyberRegs has already had a broad impact on financial institutions that are authorized to engage in business in New York ("Covered Entities"). Furthermore, even for those financial services companies not directly covered, the CyberRegs has generally raised the expectations of other regulators and defined what are considered best practices for cybersecurity programs in the industry. We briefly discuss below five things that general counsel ("GCs") should understand about the CyberRegs and their organizations' compliance with the requirements.

Annual Board Report and Certification

At least annually, the chief information security officer ("CISO") is required to provide a report to the Covered Entity's board or other governing body on the cybersecurity program and material cybersecurity risks, considering, as applicable, material cybersecurity events and the overall effectiveness of the program. Additionally, the board of directors (or one or more of the senior officers of the Covered Entity) are required to certify the Covered Entity's compliance with the CyberRegs to the NYDFS on an annual basis by February 15 of each year.

GCs of Covered Entities should understand the annual reporting and certification obligations. This may include determining whether the annual report is being made to the board of directors and whether the board is actually engaging the CISO or management on the report's content. GCs also should understand who within their organization is certifying compliance with the CyberRegs and what procedures are in place to ensure that those individuals providing the certification have the information needed to support the compliance certification. For some Covered Entities, these procedures may include obtaining

1. NYDFS, *Cybersecurity Requirements for Financial Services Companies*, XXXIX (No. 9) N.Y. Reg. 3 (Mar. 1, 2017) (*codified at* N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500).

sub-certifications or other similar assurances from employees with direct knowledge and responsibility for the key elements of the cybersecurity program.

Breach Notification

A Covered Entity is required to put in place a written incident response plan designed to enable the organization to promptly respond to and recover from a cybersecurity event materially affecting the confidentiality, integrity or availability of its systems. As part of this plan, Covered Entities are required to notify the NYDFS within 72 hours after becoming aware of any cybersecurity event with a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" or for which notice must be provided to any government body, self-regulatory agency or other supervisory body.

GCs of Covered Entities should understand how their CyberRegs notification procedures are integrated into pre-existing 50-state breach notification procedures set out in the incident response plan. They also should ensure that the incident response plan identifies the person or group of individuals responsible for deciding whether an incident is subject to the CyberRegs notification requirement and making sure that this decision-making process involves the GC or another lawyer.

Third-party Service Provider Compliance

Beginning in March 2019, the CyberRegs will cause Covered Entities to pass on certain cybersecurity obligations to third-party service providers ("TSPs") by requiring Covered Entities to develop written policies and procedures designed to ensure the security of systems and data accessible to, or held by, TSPs. Additionally, each Covered Entity will be required to address with their TSPs through due diligence or contractual protections (i) the use of access controls and multi-factor authentication, (ii) encryption of nonpublic information in transit and at rest, (iii) prompt notification to the Covered Entity of certain cybersecurity events and (iv) representations and warranties from the TSPs concerning their cybersecurity policies and procedures.

GCs of Covered Entities should consider whether their company has updated its contractual terms for TSPs to include the required contractual protections contemplated by the CyberRegs. For example, do the Covered Entity's contracts require notice of the types of "cybersecurity events" covered by the CyberRegs and in a time and

manner that would enable the Covered Entity to satisfy its notification obligations to the NYDFS (as described above)? GCs also should understand how procurement personnel (including lawyers and stakeholders) and others within the organization evaluate new TSPs and monitor the activities of existing TSP relationships and activities for compliance with the CyberRegs.

Data Governance and Classification

The CyberRegs states that a Covered Entity's cybersecurity policy must address data governance and classification but does not define those two terms. We think this provision refers to the need for a Covered Entity to be aware of the types of information it possesses and to implement a framework that is designed to ensure that nonpublic information is identified and protected by the cybersecurity program.

GCs of Covered Entities should understand where their nonpublic information is stored and how data is classified within the organization (e.g., public, confidential, highly confidential). A Covered Entity cannot effectively protect its nonpublic information until it understands where the information is stored, who has access and how is it transmitted. Proper data classification is another important element of data security as providers, senders and recipients of such information will need an immediate understanding of the sensitivity of the data. GCs also should help ensure that the flows of nonpublic information within the Covered Entity are protected in a manner consistent with applicable law (including the CyberRegs).

Training

A Covered Entity's cybersecurity personnel are subject to ongoing subject-matter training requirements, and all of a Covered Entity's personnel must undergo regular cybersecurity awareness training that is updated to reflect risks identified in its periodic risk assessment. Employee and vendor training is an important aspect of any cybersecurity program as employees, along with vendors, are frequently responsible for breaches and other cybersecurity incidents. Many of the breaches resulting from phishing, spearing phishing and other third-party attacks could be avoided by targeted training, and the resulting harm from successful attacks could be mitigated by conducting tabletop and similar training exercises to test the incident response plan.

GCs of Covered Entities should ask their learning/training and information security departments about the type of employee and vendor training that the organization is providing and assess whether this training meets the requirements of the CyberRegs. They also should ensure that the Covered Entity is able to demonstrate that the training being provided is related to its particular cybersecurity risks and goes beyond generalized "how to use technology" training that is often provided as part of an employee's on-boarding.

Be Aware of New State Cybersecurity Requirements

After the NYDFS adopted the CyberRegs, the National Association of Insurance Commissioners adopted an Insurance Data Security Model Law that is intended to be enacted by the legislature of each state and has already been enacted in South Carolina.[2] While the model law's requirements have strong similarities to the CyberRegs, there also are some differences, particularly with respect to insurance industry-specific structures and practices. Therefore, compliance with the CyberRegs will not necessarily ensure compliance with other states' statutes that are based on the model law. However, in our experience, insurance licensees can leverage the steps they have taken to comply with the CyberRegs to achieve compliance with the model law's requirements. We'll cover new and emerging state cyber and privacy requirements in more detail later this month as part of this series.

For more information section about the topics raised in this Legal Update, please contact any of the following lawyers.

Lawrence R. Hamilton
+1 312 701 7055
lhamilton@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

Matthew Bisanz
+1 202 263 3434
mbisanz@mayerbrown.com

2. NAIC, *NAIC Passes Insurance Data Security Model Law* (Oct. 24, 2017). The text of the Model Law, which has been designated by the NAIC as Model 668, is available at http://www.naic.org/store/free/MDL-668.pdf.

CALIFORNIA ENACTS GDPR-LIKE CONSUMER PRIVACY PROTECTIONS: WHAT YOU NEED TO KNOW

10 July 2018

Mayer Brown Legal Update

The state of California recently enacted the most sweeping general privacy statute in the United States. The California Consumer Privacy Act, codified in Assembly Bill 375 ("CCPA"), will take effect on January 1, 2020, and is intended to give California consumers more control over their personal information and how it is collected, used and sold by companies. The CCPA was modeled on the California privacy ballot initiative that was set to be voted on in November (but has since been withdrawn) and applies to companies of a specific size or engaging in certain activities in California.

Coverage of the CCPA

Unlike existing state and federal privacy laws, which tend to focus on a specific sector or type of personal information, the CCPA applies across industries and to a wide range of consumer information, providing protections to a significant numbers of consumers. The CCPA covers for-profit companies doing business in the state of California that satisfy one of the following criteria: (1) has annual gross revenues in excess of $25 million (as adjusted), (2) annually buys, receives, sells or shares personal information for commercial purposes of 50,000 or more consumers or (3) derives 50 percent or more of its revenues from selling consumers' personal information.

While service providers[1] are not expressly covered, companies face certain restrictions on the "selling" of personal information to third parties. The CCPA exempts from those restrictions the sharing of personal information for business purposes with a service provider if (1) the company has provided sufficient notice to the consumer of this sharing and (2) the service provider does not further collect, sell or use the personal information except as necessary to perform the

1. Defined in the CCPA as an entity "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purposes pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purposes other than for the specific purpose of performing the services specified in the contract for the business…".

business purposes. Furthermore, the CCPA excludes from the definition of "third party" those parties with whom the company shares personal information for a business purpose and pursuant to a contract meeting certain identified conditions. Companies will need to review their contracts with service providers and make any necessary changes before the effective date.

Key Components of the CCPA

The CCPA imposes a number of new obligations that go beyond what is generally required or expected under existing federal or state privacy laws. To date, US privacy laws have focused on requiring disclosures regarding companies' information practices, enforcing the commitments made to consumers regarding those practices and restricting sharing consumer information with unaffiliated third parties for marketing purposes.[2] Recent attention to data issues at the state level have focused largely on information security and notice in the event of unauthorized access rather than providing consumers with additional rights with respect to the collection, use, sharing or sale of personal information. The CCPA, therefore, is a departure from the approach of most current US privacy laws in its focus on providing consumers with new rights and protections with respect to broad categories of personal information collected about them. While a few recent laws, such as the New York Department of Financial Services cybersecurity regulation, have included somewhat similar provisions aimed at limiting data retention, the CCPA will significantly alter the current framework in the US regarding consumer access and the retention of information.

While the CCPA's focus on consumer rights has drawn comparisons to it and the EU General Data Protection Regulation ("GDPR"), companies should not assume that by extending their GDPR compliance to California they will satisfy the state's new law. Although a company with a GDPR compliance program will find it easier to adapt to the CCPA, key differences between the rights granted by each law will require companies subject to the CCPA to closely evaluate the new law and to ensure that they have the operational, technical and contractual ability to effectuate the rights of consumers with regard to

2. While Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act broadly addresses consumer access and portability of certain financial information, no implementing regulations were issued.

any personal information they collect. Additionally, the GDPR introduces new restrictions on certain processing and imposes recordkeeping and other obligations as part of a company's general privacy compliance program that are not specifically required by the CCPA.

The key components of the CCPA:

1. **Broader definition of "personal Information"**: Unlike many privacy statutes in the United States, the CCPA uses a very expansive definition of personal information to include "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Specific categories addressed in the CCPA include, among other things, unique identifiers, biometrics, geolocation data, browsing and search information, and "inferences drawn" from such personal information that are used to create a profile about a consumer. The definition excludes de-identified or aggregate information or information that is publicly available from federal, state or local government records.
2. **New disclosure requirements**. The CCPA gives consumers the right to request that a company disclose the categories and specific pieces of personal information it has collected about them in the past 12 months, as well as information about that data—the source of the information, what a company does with it and the categories of third parties with which it shares the data. Consumers can make such requests no more than twice a year and at no charge to them, and companies must respond to verifiable requests within 45 days, which can be extended. Although similar to California's current "Shine the Light" law, the CCPA imposes disclosure obligations on a much broader set of companies and applies to a broader set of data processing activities compared to the "disclosure" of personal information for direct marketing purposes requirements of the "Shine the Light" law.
3. **New right to delete**. The CCPA gives consumers the right to compel companies to delete personal information "collected from the consumer." There are certain exceptions to this, including data collected to protect against fraud or other illegal activity, enable internal uses that are reasonably aligned with consumer expectation and complete a business transaction with the consumer. Complying with the new rights to delete and disclose data may require companies to make certain operational changes to how they store

and process personal information, as well as make changes to their vendor agreements.

4. **New restrictions on sale of data**. The CCPA gives consumers the right to opt out of the sale of their personal information, and companies must obtain opt-in consent from anyone under 16 years of age (which must come from parents or guardians if the consumer is under the age of 13). While opt-out rights are standard under the Gramm-Leach-Bliley Act, the California Financial Privacy Act and the GDPR require that consumers opt in to certain types of sharing. The CCPA defines "sale" as "the selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." (Sec. 1798.140(t)(1).)

5. **New privacy policy requirements**. Companies must also, prior to data collection, provide notice to consumers in privacy policies about their data practices and are prohibited from collecting additional personal information or using existing personal information collected for an additional use without notice to consumers. Companies must make it easy for consumers to facilitate the rights provided in the CCPA by describing to consumers the methods they can use to make requests of companies, covering other information in their policies and placing "Do Not Sell My Personal Information" buttons on their websites.

6. **No discrimination**. Companies are prohibited from discriminating against consumers for exercising any of the rights provided for in the CCPA, including by denying goods and services, charging different prices or providing a different level of quality of their goods and services. There is an exception if the difference in price, level or quality of goods and services is reasonably related to the value provided by the consumer's data. Companies are allowed to offer financial incentives for the collection and sale of their personal information as long as they are not "unjust" or "usurious." This may enable companies to offer discounts on products or services to consumers who will allow their information to be used by, shared with or sold to third parties, but there is uncertainty regarding how the California attorney general will interpret and enforce this restriction.

7. **Impacts to already regulated companies**. While the CCPA provides for certain exemptions for personal information governed by certain federal statutes (specifically the Health Insurance Portability and Accountability Act,[3] the federal Fair Credit Reporting Act, the Gramm-Leach-Bliley Act and the Driver's Privacy Protection Act), those exemptions apply only to the personal information that is covered by those statutes and not to the entire company subject to them. Furthermore, some of the exemptions in the CCPA apply only to the extent that the federal law conflicts with the CCPA. While the Fair Credit Reporting Act contains provisions preempting certain types of state laws, the Gramm-Leach-Bliley Act does not generally preempt state laws affording consumers greater protections. The interplay between existing federal privacy laws and the CCPA will require a detailed analysis, and many companies will need to consider their compliance with the CCPA even if they already comply with sector-specific federal data privacy laws.
8. **Enforcement by the attorney general**. The CCPA is enforced by the California attorney general and any person, business or service provider found in violation of it could be penalized up to $7,500 per incident. The CCPA requires the attorney general to provide the entity with written notice of the violation along with a 30-day period to address the non-compliance.
9. **Private right of action**. In addition to enforcement by the California attorney general, the CCPA provides California consumers with a limited private right of action in connection with a breach of non-encrypted or non-redacted personal information resulting from a violation of reasonable security practices and procedures. The CCPA requires that, before proceeding with a lawsuit, a consumer must give the company 30 days' notice to cure the violation, as well as provide notice to the California attorney general, who will decide whether to bring charges themselves or let the consumer proceed.

3. However, the text of the CCPA misidentified HIPAA as the Health Insurance Portability and *Availability* Act.

10. **Future changes**. Future amendments and clarifications to the CCPA are likely. Lawmakers in California are expected to amend the law before its effective date on January 1, 2020. The ability of lawmakers to make such amendments through the regular legislative process was a key reason why industry gave its support to the state legislature passing the CCPA within only a week of its introduction since, by doing so, the lead sponsor of the November ballot initiative agreed to its withdrawal ahead of the June 28 withdrawal deadline. The November ballot initiative could not have been similarly amended through the regular process had it been passed into law. Separately, the statute also instructs the California attorney general to develop and adopt regulations ahead of the effective data in a number of specific areas identified in the CCPA that are necessary to further the purposes of the CCPA. Providing the California attorney general with rulemaking authority could ultimately provide greater protections to consumers and more stringent obligations on covered businesses.

ePRIVACY REGULATION: WHAT TO EXPECT (AND WHEN) OR WHY DOES IT TAKE TWO (OR EVEN THREE) TO TANGO?

22 June 2018

Mayer Brown Legal Update

GDPR Day (i.e., May 25, 2018) has passed, bringing with it higher standards for data privacy, but there is more to be done: the European Union ("EU") is working hard to finalize its reform of the ePrivacy Directive, an effort initiated in January 2017 when the EU Commission adopted a proposal for a Regulation on Privacy and Electronic Communication (the "ePrivacy Regulation" or the "Regulation").

In a nutshell, the ePrivacy Regulation is *lex specialis* to the General Data Protection Regulation ("GDPR"). While the GDPR applies to all categories of personal data—hard copy and electronic—the ePrivacy Regulation would typically only apply to electronic communications data, a subset. The Regulation, if adopted, would cover not only traditional telecommunications operators and providers of electronic communication services but also "over-the-top" communications services. (For an outline on what the ePrivacy Regulation contemplates, see our *The European Files article* (p. 24).)

While the policymakers had hoped that the ePrivacy Regulation would enter into force on GDPR Day, this obviously didn't happened. However, certain actions have been taken to push the ePrivacy Regulation forward: on GDPR Day, both a progress report was issued by the presidency of the Council (the "Progress Report") and a statement was issued by the European Data Protection Board ("EDPB"), the successor of the Working Party No. 29. The ePrivacy Regulation was debated on June 8, 2018, by the Transport, Telecommunications and Energy Council ("TTE") and subsequently re-discussed at a technical level on June 14, 2018.

Below we provide a summary of these recent developments and a prospective timeline for the adoption of the ePrivacy framework.

Progress Report

The Progress Report reflects the intense work that has taken place since the beginning of 2018. It relays concerns expressed at a political level and outlines suggested changes to the initial ePrivacy Regulation resulting from discussions between representatives of various EU member states. It's particularly noteworthy that the need to inform end-users of privacy settings offered by software permitting

electronic communications is softer under the compromise text attached to the Progress Report. Indeed, software providers are only obliged to inform end-users about privacy settings at the time of installation or first usage or when updates change the privacy settings. Furthermore, the Progress Report suggests that activities concerning national security and defense be excluded from the ePrivacy Regulation. Those proposals go hand in hand with others in the Progress Report promoting increased access to end-users' terminal equipments.

The direction suggested in the Progress Report somewhat departs from the approach promoted by the European Parliament back in October 2017.

Statement of the EDPB

The EDPB states that the ePrivacy Regulation should be based on "broad prohibitions, narrow exceptions, and the use of consent." The EDPB points out, as the European Parliament has, that the confidentiality of electronic communications requires a more extensive protection than the one offered by the GDPR and that consent from end-users should be obtained systematically. The EDPB criticizes the possibility to process electronic communications content and metadata based on open-ended grounds, such as the organization's "legitimate interests" or the general purpose of performing a contract. In the same context, the EDPB says that processing electronic communications metadata without consent should only be done after the data has been anonymized.

The EDPB states that the ePrivacy Regulation should apply as soon as data relating to the behavior of a user are collected, whether or not the user has created an account for a service. According to the EDPB, this approach will ensure the protection of the user's privacy while permitting fair competition between data controllers.

The EDPB advises that the ePrivacy Regulation enforce consent requirement for cookies and similar technologies. In line with the European Parliament's view, the EDPB supports the application of privacy by default standards. It states that privacy settings should allow users to give and withdraw consent in an easy, binding and enforceable manner against all parties. The EDPB believes that such an approach should explicitly apply to the operating systems of smartphones, tablets and any other "user agent"—i.e., that communications applications should take into account users' choices, no matter what technical means are involved.

What's Next (and When)?

The TTE Council did not tackle all of the issues raised in the Progress Report and the EDPB's statement. According to information made publicly available, the TTE Council merely stressed the need to have a balanced text, "user friendly and future proof." Given the variety of positions expressed by the TTE Council, the European Parliament and the EDPB, further discussions will be necessary to reach to an agreement, delaying in the adoption process.

To illustrate that, following the political debate on June 8, 2018, the presidency of the Council didn't even introduce changes to the ePrivacy Regulation in preparation for the technical discussions held on June 14, 2018 at the level of the working party. Rather, it proposed various options and directions for the member states to first consider and agree on. Time is pressing, however, as the upcoming European elections in 2019 are very close and might put the whole adoption process on hold.

Under EU law making processes, it can take as many as three to tango, which makes for a challenging set of steps.

INTERNATIONAL DEVELOPMENTS IN PRIVACY LAWS AND VENDOR AGREEMENTS

By Authors Lei Shen, Oliver Yaros, Qi Chen, and Daniel Gallagher[1]

Cybersecurity and data privacy increasingly have been a topic of focus around the world, and developments in this realm are increasing at a rapid rate. Several countries have recently implemented new laws and regulations focusing on data protection. These developments will have an impact not only on how companies operate, but will also affect what they need to include in their agreements with their third-party vendors that have access to personal data. Below are some of the recent developments in the United States, the European Union, and the Asia-Pacific region.

Developments in the United States

STATE LAWS

In 2017 and early 2018, several states moved forward with legislation addressing security and data privacy concerns. In March 2018, Alabama became the 50th state to enact a data breach notification law, which, like a small group of others, imposes a specific notification deadline of 45 days after the discovery of a breach. A number of states have broadened the definition of personal information (e.g., a user name and password) in their state laws in recent years. Since many national and international companies do not distinguish data by state residency, when data that are subject to different state requirements are intermingled, companies must observe the strictest state standards for all of the data. On the privacy side, Washington State became the third state—after Texas and Illinois—to enact a law regulating the commercial collection and use of biometric information.

1. Lei Shen is a partner in the Cybersecurity & Data Privacy and Technology Transactions practices in Mayer Brown's Chicago office. Oliver Yaros is a partner in the Intellectual Property & IT Group of the London office, having joined Mayer Brown as a trainee in 2004 and admitted to practice in 2006. Qi Chen is an associate in the Technology Transactions practice in Mayer Brown's Chicago office. Daniel Gallagher is a senior associate in the London office of Mayer Brown's Intellectual Property and Technology Transactions practices, as well as the Cybersecurity & Data Privacy practice.

NEW YORK STATE FINANCIAL SERVICES REGULATION

The New York State Department of Financial Services (NYDFS) adopted a cybersecurity regulation that mandates cybersecurity standards for all institutions authorized by NYDFS to operate in New York, including many banks, insurance entities and insurance professionals. Significant provisions of the cybersecurity regulation became effective in 2017, and other provisions will be phased in throughout 2018 and 2019. The cybersecurity regulation is quite comprehensive and addresses everything from access controls and encryption to data disposal and employee training. It requires covered entities to report to NYDFS on the occurrence of a broad range of cybersecurity "events" that include attempted or successful data breaches, security incidents, hacking and intrusions. It also includes requirements for third-party service providers. Following the enactment of the final cybersecurity regulations for New York's financial services sector, state financial regulators in Colorado and Vermont adopted their own cybersecurity rules that would apply to certain entities doing business in their states.

Developments in the European Union

GDPR

The new European General Data Protection Regulation (GDPR), which will replace EU Data Protection Directive 95/46/EC (EU Directive) on May 25, 2018, will bring with it a number of significant changes from the EU Directive, including significant fines, breach notification requirements, a change in jurisdictional scope, new data subject rights and direct processor requirements. Even businesses that are established outside the European Union will be subject to the GDPR as data controllers if they process personal data in relation to the offering of goods or services to individuals within the European Union or to the monitoring the behavior of individuals in the EU. Accordingly, businesses that previously were not subject to the EU Directive may become subject to the GDPR.

Under the GDPR, businesses must notify the relevant EU data protection authority of a data breach without undue delay and, where feasible, within 72 hours (unless the breach is unlikely to result in a risk to the individuals concerned). They must also notify individuals of a data breach without undue delay if a breach is likely to result in a high risk to the individuals concerned.

The GDPR will introduce significant other changes and additional requirements that will also need to be addressed by businesses, such as data subjects' "right to be forgotten," the requirement to implement data protection by design and by default, and the requirement for data protection impact assessments.

To address concerns regarding how to comply with the various new requirements, several data protection authorities, as well as the A29WP, have been releasing and will continue to release guidance concerning the GDPR. For example, the A29WP has released guidelines on the right to data portability, data protection officers (DPOs), data protection impact assessments (DPIAs), data breach notification, and other topics. The UK's ICO has also released draft guidance on contracts between controllers and data processors and how to obtain consent under the GDPR. Additional guidance is expected in 2018.

NIS Directive

The EU Network and Information Systems Directive 2016/1148 (NIS Directive) will also take effect in 2018. The NIS Directive requires providers of essential services (which, for the purposes of the NIS Directive, are services that are essential for the maintenance of critical societal and/or economic activities that rely on network and information systems, which, if subject to a cybersecurity incident, would have a significant disruptive effect on the service) or digital services with an establishment in the European Union (or not established within the European Union but offering an online marketplace, search engine or cloud computing service in the European Union) to notify of cybersecurity incidents to the relevant authority without undue delay if those will have a significant (essential services) or substantial impact (providers of an online marketplace, search engine or cloud computing service) on the continuity of the services being provided.

Developments in the Asia-Pacific Region

While many countries in the Asia-Pacific region have lagged behind North American and EU countries with respect to cybersecurity and data privacy in the past, recent developments show that countries in this region are starting to make significant changes in this area.

CHINA AND THE CSL

One big development is China's enactment of its new Cybersecurity Law (CSL), the first comprehensive law in the country's history to focus on cybersecurity. The CSL took effect in June 2017. The law is

controversial as it may require data collected or generated in China during business operations to be stored in China unless the entity subjects itself to a security assessment and shows that cross-border transfer of the data is necessary for its business. Many of the details on the data localization requirement (such as exactly which entities must comply with the requirement) are still ambiguous, and China is expected to release new measures and specifications related to the CSL in the future to clarify these ambiguities. China released one such specification in December of 2017 called the "Information Security Technology – Personal Information Security Specification" (PI Specification). The PI Specification is not mandatory but provides detailed guidance on the collection, storage, use, transfer and disclosure of personal information, as well as organizational standards and data breach responses for personal data controllers, which will likely be referenced by Chinese regulators in their enforcement of the CSL. The contents of the PI Specification generally reflect the requirements of personal information standards adopted by other jurisdictions around the world (e.g., consent to collection of personal information and obligation to protect the personal information collected). While many have criticized the data localization requirement in the CSL, it appears other countries in the region, such as Vietnam, are also considering similar requirements in their draft cybersecurity laws.

OTHER DEVELOPMENTS IN THE ASIA-PACIFIC REGION

Other countries across the Asia-Pacific region are also moving toward tighter regulations and stronger enforcement with regard to cybersecurity and data privacy.

Korea is requiring service providers to obtain permission before accessing data or functions on a user's smart phone, and such providers may not deny service to users if the user refuses to give permission for data or functions that are not necessary to the provision of the service.

India is expanding the definition of cybersecurity incidents to include attacks in addition to actual breaches and is moving toward requiring all businesses to report cybersecurity incidents to the Computer Emergency Response Team (CERT), India's official cybersecurity agency.

Australia passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016 in February 2017 requiring organizations to immediately notify the Office of the Australia Information Commissioner and the affected individuals of data breaches that are likely to result in serious harm. The amendment will take effect in February 2018.

Smaller countries have also been active in the cybersecurity and data privacy area. Singapore and Vietnam both released comprehensive draft cybersecurity laws for public consultation in 2017. Taiwan is deliberating a bill to require providers of its critical infrastructures to develop information security plans and notify the authorities in the event of security breaches. Indonesia established its first national cyber agency in June through a presidential regulation.

Updates to Vendor Contracts

In light of the developments above, agreements with third-party vendors that will have access to your personal data should be reviewed in order to ensure that they comply with these developments in data protection laws. Below are some of the issues that should be considered when undertaking a review of your vendor agreements.

GDPR

The most significant issue that you will need to consider is whether you are subject to the GDPR and whether your vendors will be processing EU personal data on your behalf. If so, you will need to revise your vendor agreements to comply with the GDPR—in particular, its Article 28, which sets out a list of items that data controllers must include in their contracts with vendors that process EU personal data on their behalf. If your agreements already comply with the EU Directive, some of the requirements of Article 28 may already be adequately dealt with (for example, that the processor only processes personal data on the documented instructions of the controller and that it has appropriate security measures in place). The new requirements for contracts with vendors that process EU personal data on your behalf include the following:

- The contract must include a description of the subject matter and the duration of processing, its nature and purpose, as well as the types of personal data being processed in respect of which categories of data subjects.
- There must be an obligation on the vendor to assist you with your obligations under Articles 32 to 36 of the GDPR, which include assisting you with notifying a supervisory authority or a data subject of a data breach and conducting data protection impact assessments.

- The vendor must agree to assist you so that you can comply with your obligations with respect to requests from data subjects that are exercising their rights under the GDPR.
- The vendor must make available to you all information necessary to demonstrate compliance with its obligations under Article 28 of the GDPR and must allow for and contribute to audits by you or another auditor mandated by you.
- The vendor must ensure that all of its personnel who process personal data are bound by confidentiality obligations.
- The contract must require the vendor to delete or return (at your option) all of the personal data at the end of the services relating to such processing and to delete any existing copies of the personal data (unless otherwise required by EU law).

In addition to the above, you should also review and consider whether other provisions need to be updated to reflect the GDPR's requirements, including data transfer restrictions and liability provisions, to address the increased potential fines under the GDPR.

DATA BREACH NOTIFICATION REQUIREMENTS

Several new laws and regulations, including the GDPR, add new data breach notification requirements. For example, the GDPR adds data breach notification requirements for both data controllers and data processors. You may need to update your vendor agreements to include data breach notification requirements or update the time frame in the agreement to ensure the vendor notifies you with enough time for you to meet your own notification requirements.

CYBERSECURITY REQUIREMENTS

You may also need to update your vendor agreements to ensure that your vendors meet certain minimum cybersecurity requirements. You may also want to consider drafting your own minimum security requirements that your vendors must meet to handle your data.

DATA LOCATION

Finally, you may want to require that the vendor only store and process your data within certain jurisdictions, both to address any data localization requirements and any data transfer restrictions.

NOTES

NOTES

32

Hunton Andrews Kurth Client Alert: Privacy and Data Security Due Diligence in M&A Transactions (May 2017)

Submitted by:
Lisa J. Sotto
Aaron P. Simpson

Hunton Andrews Kurth LLP

Client Alert

May 2017

Privacy and Data Security Due Diligence in M&A Transactions

Privacy and data security issues have become the subject of critical focus in corporate mergers, acquisitions, divestitures and related transactions. In 2016 and 2017, several large transactions, especially those involving telecommunications, entertainment and technology companies, have been impacted by either concerns about the collection and use of personal information or significant information security breaches. The Federal Trade Commission has sharpened its focus on the use of personal information as a factor in evaluating the competitive effects of a given corporate transaction, and the Securities and Exchange Commission is now closely scrutinizing privacy and data security representations made to investors in public filings connected to transactions. More broadly, privacy and data security problems that are not timely discovered before entering into an M&A transaction can become significant liabilities post-closing and also lead to litigation.

The Importance of Thorough Due Diligence

Because of this heightened concern, it is imperative that companies conduct thorough due diligence about privacy and data security issues before entering into a transaction. The goals of the due diligence process should be to help the parties in a transaction understand (1) what promises and representations a company has made with respect to privacy and data security; (2) whether a company needs to obtain any consents from consumers, employees or others post-transaction to be able to use the personal information previously collected; (3) how the parties' information security programs are structured; (4) how the company has responded or could potentially respond to significant data breaches; and (5) the buyer's potential liability for privacy and data security issues post-closing.

To accomplish these goals, companies should prepare a comprehensive privacy and data security due diligence checklist that it can use for a variety of transactions. The checklist should (1) ask specific questions about privacy and data security issues, such as the types of personal information collected, the parties that may access such information and how such information is transferred within and outside the organization and (2) request relevant privacy- and security-related materials such as privacy notices, information security policies and procedures, incident response plans, privacy and information security training materials, contracts with third-party service providers and any internal and external privacy compliance reviews, assessments or audits.

The due diligence checklist should be customized based on the profile of the target entity and the industry in which it operates. If personal information is at the heart of a transaction, the checklist will usually be quite granular and may involve the provision of ancillary documents such as data flow maps. In addition, certain types of companies such as health care providers and financial institutions must consider sector-specific rules that may impact the nature and structure of the transaction. Finally, the due diligence should also reflect scope, risk tolerance and timing considerations.

Any limitations on due diligence will need to be addressed, such as via the inclusion of more stringent privacy and data security provisions, in the transaction documents. This may include specified indemnities and an escrow account to address potential post-closing liabilities. Limited due diligence also

raises the importance of disclosure schedules — inadequate or incomplete disclosure schedules make it difficult for companies to evaluate the risks associated with a transaction.

Lessons Learned

Companies that fail to conduct proper due diligence into privacy and data security issues in advance of a transaction may run into significant problems following the transaction. These problems may create financial liabilities or prohibit the buyer from using or disclosing customer personal information. Even more impactful, companies may be saddled with material costs related to privacy and data security, such as costs associated with data breach class action litigation, shareholder derivative litigation or government investigations. These post-closing costs often have the potential to destroy any cost-saving synergies that were the impetus for doing the deal in the first place.

Hunton Can Help

Hunton has created a cross-disciplinary legal team dedicated to guiding companies through the minefield of regulatory and cyber-related risks associated with high-stakes corporate mergers and acquisitions. The new team brings together the firm's renowned capabilities in privacy and cybersecurity with its recognized strength in M&A transactions.

Contacts

Lisa J. Sotto
lsotto@huntonAK.com

Steven M. Haas
shaas@huntonAK.com

Aaron P. Simpson
asimpson@huntonAK.com

Allen C. Goolsby
agoolsby@huntonAK.com

Ryan P. Logan
rlogan@huntonAK.com

Brittany M. Bacon
bbacon@huntonAK.com

**As of April 1, 2018, Hunton & Williams is now Hunton Andrews Kurth.*

NOTES

NOTES

33

Legal and Business Issues in AI, Big Data and IoT—A Practical Checklist

Lisa R. Lifshitz

Torkin Manes LLP

Prepared by Lisa R. Lifshitz, Partner, Business Law Group and leader of the Technology, Privacy and Data Management and Emerging Technology Groups, Torkin Manes LLP, Toronto, available at (416) 775-8821 or by email at llifshitz@torkinmanes.com.

PRIVACY/DATA ISSUES

- ✓ AI requires the gathering of immense amounts of data and the sharing of data to oversee it. Did the AI developer (or entity the AI developer licensed data from) have sufficient rights or obtain the necessary (and meaningful) consent to collect the original data?
- ✓ Did the AI developer have the rights to use and process the data collected, create derivative works using the data, and additionally disclose the data?
- ✓ Did the data come with "strings attached" on how it can be used?
    - ○ patient data under the Health Insurance Portability and Accountability Act of 1996 (HIPPA).
    - ○ non-public personal information under the Gramm-Leach-Bliley Act.
    - ○ The EU General Data Protection Regulation (GDPR).
    - ○ Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and other substantially similar provincial private sector and provincial health privacy laws and other laws.
- ✓ Who owns the data generated by the device/system?
- ✓ How anonymized/de-identified is such data?
    - ○ How much effort will it take to re-identify individuals' data?
- ✓ How can one meaningfully consent to the collection, use and disclosure of data obtained through use of the IoT device?
    - ○ Insufficient information is provided to allow individuals to exert control and provide meaningful consent.
- ✓ Consider sensitivity of users using the devices.
    - ○ Children and "smart" IoT toys [i.e. Germany's Federal Network Agency has banned a smart doll called My Friend Cayla after deeming it a hidden spy device.]
        - ▪ "Smart Toys" collect considerable amounts of data to function, including data about an internet connection (IP address, login credentials), personal information about a child for registration (full name, gender, date of birth, etc.); data provided during communication with a child (voice recordings, photos, videos, voice and text messages, etc.);

data about parents (phone number, location, credit card information, etc.).

- Patients and medical devices.

✓ Consider the intersection of privacy laws, AI/IoT in the US and abroad.

- GDPR, Canada, India, Singapore.
- Transparency problems – what is meaningful consent in the context of a decision made by an AI?
- Is existing legislation sufficient or is specialized AI/IoT legislation required?[2]

✓ Increased direct collection of "sensitive" personal information by IoT devices, such as precise geo-location coordinates, financial account numbers and health information (i.e. Fitbits, Apple watches notifying users of medical emergencies).

✓ Concerns re IoT devices and data collection.

- No anonymity.
- Increased opportunities for businesses to monitor consumers and monetize data.
- Content recording (spending habits, behaviors, voice patterns, daily activities).
- Audio and video recording, voice patterns.
- Existing smartphone sensors can be used to infer a user's mood; stress levels, personality type, bipolar disorder, demographics (e.g. gender, marital status, job status, age), smoking habits, overall well-being, progression of Parkinson's disease, sleep patterns, happiness, levels of exercises and types of physical activity or movement.

✓ Inferences can be used to provide beneficial services to consumers, but can also be misused – i.e. by companies that use such data to make adverse credit, insurance and employment decisions.

---

2. For example, see California's Senate Bill 327, chapter 886 and Assembly Bill No. 1906, "Security of Connected Devices". For more information, see "*Security by design: California's new IoT security laws*", *Canadian Lawyer online* (November 19, 2018) available at https://www.canadianlawyermag.com/author/lisa-r-lifshitz/security-by-design-californias-new-iot-security-laws-16511/.

- i.e. using fitness tracker data to price health or life insurance or to infer the user's suitability for credit or employment.

✓ Given mandatory federal/state/provincial data breach/breach of security safeguards' legislation, consider obligations of IoT device manufacturers, AI systems' developers to notify end users regarding unauthorized data disclosures.

- that create a 'real risk of significant harm' (Canada – PIPEDA, Alberta PIPA)
- The California Consumer Privacy Act
- Other state breach laws.

SECURITY ISSUES

✓ What are the minimum security requirements for IoT devices?

- Generally no minimum standard for security for AI/IoT.
- Myriad flaws, including the use of (i) insecure communications; (ii) hardware and firmware flaws; (iii) software vulnerabilities; (iv) weak authentication or its absence altogether; (v) insecure internet connections; and (vi) insufficient protection of collected data.

✓ How do you build "privacy by design" into an AI/IoT device?

- Security is often an 'after-thought'.
- Multiple systems from different manufacturers in one IoT device.
- Use of Open Source Software in IoT devices that may be insufficiently patched/upgraded.

✓ How do you ensure that security can be kept current on an IoT device?

- The low cost of many IoT devices may also be a disincentive to IoT manufacturers from issuing security patches.
- How does a consumer get an update? Does the IoT manufacturer have a direct connection with the consumer?

✓ IoT companies should continue to monitor products throughout the products' life cycle and, to the extent feasible, patch/mitigate known vulnerabilities.

- Unfortunately, many IoT devices have limited life cycles, resulting in a risk that consumers will be left with obsolete devices that are vulnerable to critical, publicly known security or privacy bugs.
- Companies should carefully consider if they decide to limit the time during which they will provide security updates and should be transparent in their representations about providing ongoing security updates and software patches.
- Companies that provide ongoing support should notify consumers about known security risks and solutions, including updates.

✓ How do you prevent malware and hacking of IoT devices/AI systems?

✓ What happens if a company that produces AI-enabled devices then goes out of business?

- Who bears the burden of security and safety? Ongoing security patching?
- Will car makers be required to maintain the AI software throughout the lifetime of the car and multiple owners?

✓ Companies should ensure they retain service providers that are capable of maintaining reasonable security and provide reasonable oversight to ensure that those service providers do so (or face an FTC law-enforcement action).

✓ Companies should implement for systems with significant risk a 'defence-in-depth' approach where security measures are considered at several levels.

✓ Consider implementing reasonable access controls to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network — including employing strong authentication, restricting access privileges, etc.

REGULATORY ISSUES

✓ Consider areas of concern for Regulators

- Unfair/deceptive trade practices.
- Failure to meet mandatory breach notification/reporting requirements.

- ✓ How can Regulators ensure that black-box algorithms are high quality—that is, that they do what they say, and that they do it well and safely?
- ✓ How can AI/IoT manufacturers defend themselves against technical audits from Regulators? How much must be/should be disclosed to a Regulator?
- ✓ Who should regulate AI/IoT?
  - The AI/IoT companies themselves?
    - IBM's ethical use guidelines.
    - Partnership for Artificial Intelligence to Benefit People and Society (Google, Microsoft, Amazon, Facebook, Apple, and IBM).
    - Google, "Responsible Development of AI," 2018.
    - Microsoft, "The Future Computed: Artificial Intelligence and Its Role in Society," 2018.
  - Federal regulators?[3]
  - A special regulatory agency for AI?[4]
  - Not for Profits?
    - AI Global, IEEE, British Standard for Robots and Robotic Devices
  - State/Provincial Laws?
  - Global treaties?

LIABILITY

- ✓ Who is responsible if something goes wrong as a result of the AI/IoT device?
  - The manufacturer?

---

3. See, for example, the U.S. Federal Trade Commission's 2015 Staff Report "*Internet of Things: Privacy and Data Security in a Connected World*" (available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
4. European Parliament Resolution with recommendations on Civil Law Rules on Robotics (2015/2103 (INL)), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN.

- The distributor?
- The original programmer?
- Consumer/End user?
- Provider liable under contract of supply?
- IoT devices that are not provided under contract and that are accessible by Internet users generally.

✓ What is a reasonable standard of care for an IoT device?

- Is there a uniform standard?
- What if imperfections in the IoT device are more subtle?

✓ What is the reasonable standard of care for an AI system?

- Move toward a "reasonable AI" standard similar to "reasonable person?"
- Or does this go down the "strict liability" path – i.e. AI is always at fault and no "reasonableness" standard (see possible tort claims below).

✓ How can we hold the developer/creator of the AI system liable if we do not understand how a black-box algorithm makes decisions?

- Machine learning/deep learning techniques generally cannot tell us their reasoning, and even when they can, the results are often too complex for individuals to understand.

✓ Possible tort claims

- If there are flaws built into the algorithms themselves, or if regulation fails to ensure that algorithms are high quality, then the developers of algorithms (or technologies that rely on them) might become liable under tort law.
- In Canada, possible claims for negligent design, negligent manufacture and failure to warn.
  - Difficult to identify the 'defect' as well as proving negligence (autonomous nature of AI, complex systems).
- Courts have been reluctant to extend or apply product liability theories to software developers.

✓ Other damage claims

- Negligence

- Strict liability
- Warranty (Express or Implied)
- Fraud
- Product liability
- False or misleading representations and deceptive marketing practices under the *Competition Act* (Canada)
- Privacy breaches/breaches of security safeguards
- Personal injury, Property damages

✓ Consider whether contract liability should be decided under the terms of the AI/IoT contract.

- Breach of warranty, defective IoT device/AI system, failure to meet established standards.
  - Implied warranties of fitness for a particular purpose, merchantable quality (Sale of Goods Act, Ontario)
  - Consumer Protection Act (Ontario) and other provinces
  - Organizations prohibited from excluding liability for their owns acts or those of their representatives (Quebec CPA).
  - Prohibitions against mandatory arbitration clauses (prohibited under Ontario, Quebec, Alberta CPAs)
- IoT manufacturers, AI developers can seek to expressly disclaim representations and warranties, seek cross-indemnities from users.

✓ What are the due diligence obligations of users/buyers that want to use an AI system or IoT device?

- Is the obligation on the buyer/user to perform evaluations at the outset?
- Periodically?

✓ If machines buy and sell from one another, will consumer laws apply?

- Ownership of data, limitation of liability, governing law and jurisdiction.
- Scope of authority issues (e.g. recurring detergent payments for my smart dish washer up to maximum of $50).

- ✓ Mitigation – consider the usefulness of insurance in limiting liability for AI/IoT claims.
    - Does "standard" insurance (including cyberliability insurance?) cover risks associated with AI/IoT issues?
    - What is being insured?

ETHICAL ISSUES

- ✓ Is the AI system based on sufficient volume and variety of data?
- ✓ Has the AI software developer sufficiently validated the reliability of the software?
    - Are results consistent and correct?
- ✓ Do we understand the system sufficiently to audit it and understand how the results were achieved?
- ✓ Can we verify that the AI system is trustworthy?
- ✓ Concerns about bias?
    - What steps are being taken to reduce bias?
    - Inappropriate conclusions likely if results are not validated.
- ✓ Does the AI system meet the ethical criteria established by various international standards/bodies?
    - *The Montréal Declaration for a Responsible Development of Artificial Intelligence* (2018) identifies an ethical framework composed of core principles with additional sub-principles.
        - **Well-being Principle**: the development and use of artificial intelligence systems (AIS) must permit the growth of the well-being of all sentient beings.
        - **Respect for Autonomy Principle**: AIS must be developed and used while respecting people's autonomy, and with the goal of increasing people's control over their lives and surroundings.
        - **Protection of Privacy and Intimacy Principle**. Privacy and intimacy must be protected from AIS intrusion and data acquisition and archiving systems (DAAS).

- **Solidarity Principle**: The development of AIS must be compatible with maintaining the bonds of solidarity among people and generations.
- **Democratic Participation Principle**: AIS must meet intelligibility, justifiability, and accessibility criteria, and must be subjected to democratic scrutiny, debate and control.
- **Equity Principle**: the development and use of AIS must contribute to the creation of a just and equitable society.
- **Diversity Inclusion Principle**: the development and use of AIS must be compatible with maintaining social and cultural diversity and must not restrict the scope of life-style choices or personal experiences.
- **Prudence Principle**: Every person involved in AI development must exercise caution by anticipating, as far as possible, the adverse consequences of AIS use and by taking the appropriate measures to avoid them.
- **Responsibility Principle**: The development and use of AIS must not contribute to lessen the responsibility of human beings when decisions must be made.
- **Sustainable Development Principle**: The development and use of AIS must be carried out so as to ensure a strong environmental sustainability of the planet.[5]

- *The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems* (May 16, 2018).[6] Prepared by Amnesty International and Access Now; endorsed by Human Rights Watch and Wikimedia Foundation.
- *Declaration on Ethics and Data Protection in Artificial Intelligence* adopted by the 40th International Conference of Data Protection and Privacy Commissioners (October 23, 2018; endorsed by the Office of the Privacy Commissioner of Canada

5. Full text of the Declaration is available at: montrealdeclaration-responsibleai.com.
6. Full text of the Declaration is available at: https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf.

and the Commission d'accès à l'information, Québec, Canada).[7] Six core principles:

- **Fairness**: All AI and machine-learning technologies should be designed, developed and used in accordance with the fairness principle — consistent with their original purpose and any data collected for use with such AI systems used in a way that is not incompatible with the original purpose of their collection.
- **Continued attention and vigilance**. There must be accountability for the potential effects and consequences of AI systems, including he use of audits, continuous monitoring and impact assessments.
- **AI systems transparency and intelligibility**. There must be improvements on AI systems' transparency through a variety of means, including investing in public and private scientific research on "explainable" artificial intelligence, making organizational practices more transparent (by promoting algorithmic transparency and the auditability of systems and the provision of meaningful information) and ensuring that individuals are always informed appropriately when they are interacting directly with an AI system or when they are providing personal information to be processed by such systems (informational self-determination).
- **Ethics by design**. AI systems have to be designed and developed responsibly from the very start, applying the principles of privacy by default or privacy by design. This includes implementing adequate technical and organizational measures and procedures (proportionate to the type of system being designed or implemented) to ensure that data subjects' privacy and personal information are respected.
- **Empowerment of individuals**. While the use of AI is to be encouraged, it should not occur at the expense of human rights or the rights of individuals. This includes respecting data protection or privacy rights — including

7. See https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181121_01/.

rights to access, the right to object to processing and the right to erasure — and guaranteeing an individual's right not to be subject to a decision based solely on automated processing if the decision significantly impacts them. Individuals should always have the right to object or appeal and challenge decisions generated through the use of AI systems.

- **Unlawful biases or discrimination**. Concerns relating to unlawful bias or discrimination that may occur from the use of data in AI continue and such unintended results must be reduced and mitigated. Accordingly, developers should invest in research into technical ways to identify, address and mitigate bias, taking reasonable steps to ensure that the personal data or information used in automated decision-making is accurate, up to date and as complete as possible and providing specific guidance and principles in address bias and discrimination, promoting the awareness of individuals and stakeholders.

IP ISSUES

- ✓ If a company invests in creating algorithms, how can they protect their investment?
  - Patents?
  - Copyright?
    - Computer programs are recognized in Canada as 'literary works' within the meaning of the Canadian Copyright Act.
    - Likely the main source of protection for AI technology in Canada but still problematic as the "author" may not be a natural person.
  - Trade secret?
- ✓ Who owns the IP/data generated by AIs/IoT devices?
  - Who owns what when IoT devices interact with one another?
  - Who decides how it can be used?
  - Is opt out possible?

- Joint ownership (or at least broad licensing) for regulatory reporting requirements.

✓ Can an AI be an author or inventor?

- Only humans may be an author under U.S./Canadian copyright laws
- Only a person may file for a patent under U.S./Canadian patent law

✓ How well do current IP laws protect AI products? IoT devices?

✓ What are some of IP limitations?

- i.e. specific arrangements of data can be copyrighted but one cannot copyright the entire phonebook.

NOTES

NOTES

34

Privacy and Security Challenges of Advanced Technologies: Artificial Intelligence, Internet of Things, Big Data, and Blockchain

Stephen S. Wu

Silicon Valley Law Group

Table of Contents

I. INTRODUCTION 5
II. OVERSEEING, MANAGING, AND IMPROVING YOUR COMPANY'S PRIVACY AND SECURITY PROGRAM 7
A. Importance of Data Protection Management 7
B. Overview of Counsel's Role 8
C. Applicable Laws 9
1. Laws Specifically Governing Advanced Technologies 9
2. General Laws 13
D. Process of Implementing an Effective Security and Privacy Program 17
III. PRIVACY ISSUES RAISED BY ADVANCED TECHNOLOGIES 19
A. Greater Varieties of Personal Data Collected, Used, and Shared 20
B. Greater Volume of Personal Data 21
C. Greater Velocity of Personal Data 21
D. Issues of Veracity of Personal Data 22
E. Issues with Bridging Contexts of Personal Data Collection and Use 22
F. Greater Surveillance Capabilities 23
G. Lack of Control Over Personal Data 23
H. New Ways to Direct Marketing Messages to Data Subjects 24
I. Blockchain and Privacy 24
IV. SECURITY ISSUES RAISED BY ADVANCED TECHNOLOGIES 25
V. CONCLUSIONS 28

I. INTRODUCTION

Four fundamental truths emerge when we consider sweeping changes caused by advanced technologies:

- First, we are seeing increasingly rapid developments in advanced technologies such as artificial intelligence (AI), robotics, automated transportation, Big Data, Internet of Things (IoT), and blockchain. These new technologies are coming. And the pace of change is accelerating.
- Second, these advanced technologies will have a profound change on societies throughout the world. Some changes will lead to dramatic improvements in our lives – improved health, safety, mobility, convenience, efficiency, financial returns, and satisfaction. Some new technologies will seem like magic. Other changes may lead to what will seem to be terrible and terrifying results: authoritarianism, widespread intrusive surveillance, profound economic dislocation, job losses, hacking, data breaches, undermining the authenticity of media content, mass accidents, and more garden varieties of snake oil and unfair trade practices.
- Third, the profound changes wrought by advanced technologies will generate an enormous number of legal issues. Litigation will arise from the damage caused by negative consequences, and fights over the fruits of positive change will cause other suits. Efforts are already underway to mitigate these risks through better governance, agreements, and insurance.
- Fourth, as attorneys, all of us have a role in protecting our clients' interests and making sure that we promote a world in which businesses develop, sell, purchase, and operate advanced technologies in a way that protects customers and the public as well as their own reputations and financial health.

I recently read Kai-Fu Lee's September 2018 book *AI Superpowers: China, Silicon Valley, and the New World Order*. For those of you who don't know him, people refer to him as a "rock star" of the Chinese technology scene. A former Google, Microsoft, and Apple executive, he emigrated from Taiwan and received his education here in the U.S., which included a computer science Ph.D. from Carnegie Mellon University. He is now a venture capitalist incubating new businesses in China, and is considered a technology oracle. In January 2019, Scott Pelley interviewed Lee on the 60 Minutes television show. During that segment, Lee talked

about one of the advanced technologies covered here – artificial intelligence. In stressing its importance, Lee told Pelley this about artificial intelligence:

> I believe it's going to change the world more than anything in the history of mankind. More than electricity.

If Lee is right, and I think he is, it is time for lawyers to be prepared for sweeping changes in AI and other advanced technologies. By preparing today, lawyers can prevent future harms; promote safe, ethical, and legally compliant deployment of these technologies; and protect their clients' interests. We must even be prepared for the possibility of artificial intelligence displacing lawyers and support staff, and we must prepare for the ethical use of AI technologies in the practice of law, although that is a topic for a different publication. In any case, given the magnitude of changes Lee and others predict, the legal profession must now turn its attention and devote substantial time and attention to this looming juggernaut.

Before describing privacy and security challenges with advanced technologies, keep in mind that these technologies work synergistically. For instance, Internet of Things sensors (such as cameras and microphones) in s smart city setting, may collect vast amounts of Big Data, which the data controller/collector can then use for artificial intelligence applications to describe patterns in the data, predict future events, and make actionable recommendations. Because of this synergy, these technologies are not silos. They may work together to impact privacy or security. Accordingly, I organized this chapter by issue rather than by technology.

Section II begins with process. It offers thoughts on managing a data protection program for companies developing, selling, purchasing, and operating advanced technologies. Section III of this chapter covers privacy risks associated with advanced technologies, as well as risk mitigation measures. Section IV talks about security risks and associated risk management. Section V's conclusion summarizes the content in the chapter.

This chapter provides an overview of the privacy and security issues. The topics covered here could and do take up entire books. With the limited space available here, this chapter is necessarily only a summary intended to raise awareness and provide a general overview of advanced technologies and data protection. I assume a certain familiarity with the technologies described here. General background reading may fill in gaps concerning how these technologies work and details on exact threat vectors and controls for managing privacy and security risks. Nonetheless, briefly, the technologies covered here are as follows:

- Artificial intelligence involves machines simulating features of human intelligence, including for purposes of operating robots and automated transportation systems.
- The "Internet of Things" refers to network-connected machines that communicate with other machines which, for instance, allow for the control of "smart" devices that previously had no connectivity, ability to share data, or processing capabilities.
- "Big Data" is a term that refers to collecting, processing, and analyzing large quantities of data to describe what is going on based on the data, predict what will happen, and provide recommendations.
- Blockchain refers to a technology to create a distributed decentralized immutable ledger of activities or transactions. The integrity of the ledger is secured and verifiable through cryptographic digital signatures.

II. OVERSEEING, MANAGING, AND IMPROVING YOUR COMPANY'S PRIVACY AND SECURITY PROGRAM

Imagine that you are working as in-house or outside counsel for a business and you are acquiring hardware or software for an advanced technology system. What information do you need to help your company manage privacy practices and the company's information security function? How do you know if your company is managing privacy and security effectively?

Section II.A covers the importance of effective data protection management. Section II.B discusses the role of counsel in managing the data protection function. Section II.C briefly summarizes data protection compliance requirements. Section II.D talks about the process of implementing an effective security and privacy program.

A. Importance of Data Protection Management

A business procuring advanced technologies faces strategic risks from picking incorrect privacy and security strategies that lead to customer or public backlash or, in the case of products in the physical world, the business may endanger safety if a compromise of the product could lead to an accident.

Failed internal procedures, such as procedures for maintaining a trustworthy workforce, may lead to operational risks such as breaches caused by insiders. Privacy and data breaches may trigger lawsuits and governmental investigations, resulting in investigative and defense

costs, litigation costs, and the cost of settlements and fines. Organizations that sustain breaches face angry customers and damage to their reputations, resulting in the loss of customer and worker loyalty, further resulting in losses of revenue, profits, and ultimately shareholder/equity value.

Consequently, managing privacy and security effectively is crucial for the continued health of any business. Managers at businesses that fail to safeguard customer data may lose their jobs and may face personal legal, reputational, and business consequences.

B. Overview of Counsel's Role

Attorneys play a crucial role in data protection management functions within businesses. First, they can review applicable data protection laws and requirements and counsel their clients to facilitate compliance. Second, they frequently participate in and assist contract drafting and negotiation in connection with transactions that implicate data protection issues. Third, they handle potential liabilities and disputes relating to data protection. Fourth, they may lead investigations regarding data protection violations, incidents, accidents, or breaches. Finally, they help with data protection governance. For instance, they may establish data protection management structures within businesses; develop and implement privacy and security programs; draft or edit privacy and security policies, procedures, guidelines, agreements, and training materials; and support audits and assessments leading to attestations and certifications, such as those under the EU-U.S. Privacy Shield program, the ISO 27001[1] security audit framework, and SOC[2] reporting frameworks.

Attorneys must work together with other professionals to develop and implement data protection measures within a business involved with advanced technologies. The businesses that most effectively manage data protection make use of cross-functional teams of business line representatives, privacy professionals, security professionals,

1. International Organization for Standardization, ISO/IEC 27001:2013, Information technology—Security techniques—Information security management systems—Requirements (Oct. 1, 2013) (amended in 2014 and 2015).
2. "SOC" reports are accountants' reports based on the System and Organization Controls of the American Institute of Certified Public Accountants. U.S. SOC reports based on the AICPA's standards have international counterparts based on International Standard on Assurance Engagements (ISAE) 3402 issued by the International Auditing and Assurance Standards Board, which is part of the International Federation of Accountants.

internal auditors, and risk managers to handle specific processes, projects, and issues. For businesses developing advanced technologies, cross-functional teams may work on new products or services and integrate privacy and security "by design" proactively during the development process, rather than waiting until the end of the process to weigh in on data protection issues. In any business, teams may be involved in the investigation and response to security incidents or breaches to determine the best response strategy and to implement it.

Since data protection attorneys will need to provide advice about mixed questions of fact, law, and technology, they should learn as much as they can about the advanced technologies developed or used by their business lines to provide products or services, technologies used to secure personal information and information systems, and technologies used to monitor, detect, and report potential violations. Talking with information technology, audit, and security professionals, reading background information about different advanced technologies and security controls, and attending continuing education programs are invaluable. The American Bar Association Section of Science & Technology Law's E-Privacy Committee and Information Security Committee provide helpful learning and networking opportunities for attorneys new to data protection through publications, programs, listservs, meetings, and events. Attorneys new to data protection will find that a wealth of information is available to help them adjust to new data protection roles and responsibilities quickly.

C. Applicable Laws

Data protection attorneys need to understand the legal landscape of advanced technologies in order to promote compliance and mitigate legal risks. Businesses in the field of advanced technologies may have laws that apply directly to their technologies. They must also account for more general laws that cover their technologies.

1. Laws Specifically Governing Advanced Technologies

A number of new laws bear on information governance regarding advanced technologies. Perhaps the prime example is California's new connected device law, SB 327 and AB 1906 enacted on September 28, 2018, which will become effective on January 1, 2020.[3] This new law covers Internet of Things devices and other

3. Cal. Civil Code §§ 1798.91.04-1798.91.06.

connected devices. Under this law, manufacturers of "connected devices" must equip the devices with one or more security features. These features must be appropriate to the nature and function of the device. They must also be appropriate to the type of information collected, contained, or transmitted by the device. Finally, the security features must be designed to protect the device and stored information from unauthorized access, destruction, use, modification, or disclosure.[4] A "connected device" is "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address."[5] Authentication mechanisms, such as passwords, are deemed reasonable if each device has a unique password or the device forces a change from a default authenticator.[6]

The law covers more than just Internet-connected devices in that it covers Bluetooth devices as well, which may include ear phones and other computer accessories. On the other hand, the law may be underinclusive because a direct or indirect connection to the Internet is necessary. Some devices may connect to private networks rather than the public Internet. The definition of "connected device" apparently excludes these devices, even though their security needs may be as great as Internet-connected devices.

California also enacted a new type of law, a "bot disclosure law."[7] This new law relates to the use of software bots (automated agents), especially ones that post content on social media to distort voting behavior. It also would apply to bots that generate fake reviews to pump up a business's reputation. The law makes it unlawful for a person to communicate online with the intent to mislead another person about a bot's artificial identity for the purpose of knowingly deceiving a person about the content of the communication. It applies where the person is trying to incentivize a purchase or sale of goods or services in a commercial transaction or to influence voting.[8] No liability attaches, however, if the person clearly and conspicuously discloses the existence of the bot.[9]

---

4. *Id.* § 1798.91.04(a).
5. *Id.* § 1798.91.05(b).
6. *Id.* § 1798.91.04(b). It would have been better if the legislature required a certain strength of the password and not just any password.
7. Cal. Bus. & Prof. Code §§ 17940-17943.
8. *Id.* § 17941(a).
9. *Id.* § 17941(a), (b).

Other laws regulate autonomous driving. Automated vehicles may be robots, may be connected to the Internet, and may receive or generate large amounts of data. California's SB 1298 facilitates the operation of autonomous vehicles on California's highways and the testing of those vehicles.[10] In 2018, the California Department of Motor Vehicles adopted new regulations regarding autonomous vehicles. Under those regulations, manufacturers cannot place autonomous vehicles on public roads unless they provide the Department of Motor Vehicles "[a] certification that the autonomous vehicles meet appropriate and applicable current industry standards to help defend against, detect, and respond to cyber-attacks, unauthorized intrusions, or false vehicle control commands."[11] Most states now have autonomous vehicle laws, executive orders facilitating autonomous vehicles, or both. Manufacturers testing autonomous vehicles will need to comply with these laws and any data protection laws or regulations associated with them. Autonomous vehicle laws and truck platooning[12] laws[13] may not mention cybersecurity explicitly, but the process to prove safety sufficient to obtain a certification or other approval will likely include some showing of reasonable measures to prevent cyberattack.

Also, privacy laws affect the use of drones with cameras and other surveillance technologies. For example, California has a law that makes a user liable for invasion of privacy for trespassing onto land or in the airspace of another person without permission to capture video or audio where the invasion was in a manner offensive to a reasonable person.[14] Other states have drone privacy laws as well.

Finally, businesses using advanced automated data processing technologies with multinational operations, with customers in foreign countries, monitoring the behavior of foreign citizens, and processing data for foreign businesses should analyze whether they have compliance requirements under international and foreign data protection laws. For instance, the European Union's General Data

10. Cal. Veh. Code § 38750.
11. 13 Cal. Code Regs. § 228.06(a)(10).
12. "Platooning" is a technology that allows trucks to form ad hoc trains on highways, controlling the braking and throttling of trucks tailing a lead truck, and allowing the trailing trucks to drive closer to trucks ahead of them. Platoons increase safety and reduce fuel use.
13. *E.g.*, Cal. Govt. Code § 14107.
14. Cal. Civil Code § 1708.8.

Protection Regulation (GDPR)[15] grants individual rights to individuals whose personal data was involved in automated data processing. Article 15 of GDPR gives individuals a right of access to information about personal data collected about them. Paragraph 1(h) of Article 15 includes the right of the data subject to know about the existence of automated decision-making and "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[16] Recital 71 refers to the data subject having a right to an explanation of a decision reached by automated means.[17]

In addition to the right of an explanation, a data subject has a right of human intervention. Under GDPR Article 22, a "data subject shall have the right not to be subject to a decision based solely on automated processing" producing "legal effects concerning him or her or similarly significantly affects him or her."[18] In other words, a data subject can opt out of automated data processing, with the implication that a human must make a manual decision. This blanket opt-out right doesn't exist if automated processing is necessary for entering into or performing a contract, applicable law authorizes processing, or the data subject has explicitly consented.[19] Nonetheless, in instances of processing for contractual purposes or consent, the data controller must still provide for safeguards for the data subjects, which at least includes "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[20]

For example, if a bank covered by GDPR turns down an applicant located in the European Economic Area for a loan based on its software powered by machine learning system used to score applicants, the applicant has a right to an explanation of how the system determined that he or she was not eligible for a loan. Moreover, under Article 22, the data subject can demand that a bank official intervene, look at the results of the system, and listen

15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
16. *Id.* art. 15, para. 1(h).
17. *Id.* recital 71.
18. *Id.* art. 22, para. 1.
19. *Id.* art. 22, para. 2.
20. *Id.* art. 22, para. 3; *id.* recital 71.

to the data subject's arguments to contest the decision. These provisions don't require the bank to change the results of the process, but they do give data subjects relief from machine-only automated decisions and a process to challenge them.

The difficulty with these laws is that many machine learning[21] artificial intelligence systems are "black boxes." It may be difficult for even experts to explain how a machine learning system came up with a decision. Businesses and academics are working on this problem of machine learning explainability in part to satisfy requirements in GDPR and future laws likely to follow.

2. General Laws

General data protection laws may apply to advanced technologies. This section contains some examples of general laws that may impose privacy or security requirements on businesses developing, selling, purchasing, or operating advanced technologies. Some general privacy and security laws are applicable to specific sectors.

For instance, financial institutions purchasing IoT devices or using AI for processing customer nonpublic personal information must account for compliance with the Gramm-Leach-Bliley Act in 1999 ("GLBA"),[22] which is the main piece of federal legislation governing financial institution privacy and security practices. The GLBA requires covered financial institutions to implement processes and procedures to ensure the security and confidentiality of consumer information, protect against anticipated threats or hazards to the security of customer records, and protect against unauthorized access to such records.[23] In addition, the GLBA requires financial institutions to provide notice to consumers about their information practices, and give consumers an opportunity to direct that their personal information not be shared with certain non-affiliated third parties.[24] When financial institutions purchase or license advanced technologies, they must make sure they do not put nonpublic personal information at risk. For instance, banks should create

21. Machine learning is a type of artificial intelligence in which systems learn and improve based on inputs of data provided to train the system. In our example, a machine learning system can look at different factors of creditworthiness and help financial institutions distinguish between good risks and bad risks.
22. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
23. 15 U.S.C. § 6801(b)(1)-(3).
24. *Id.* § 6802(b)(1)(A)-(C).

secure transmission protocols with their automated teller machines to prevent interception and compromise of financial information.

Likewise, healthcare providers and their business associates obtaining and operating surgical and service robots, patient data machine learning and AI systems, and operational AI systems will need to comply with the Health Insurance Portability and Accountability Act (HIPAA),[25] the HITECH Act,[26] and regulations promulgated under them. Privacy notices will need to disclose what health information the business collects, how it uses that information, and to whom it will disclose the health information. The HIPAA Security Rule will require the business to implement reasonable and appropriate administrative, physical and technical safeguards to secure protected health information created, received, maintained, or transmitted by the business.[27] For example, a hospital operating service robots in its facility should have a policy to manage audio and video data recorded by the robots. It may seek to minimize the amount of protected health information recorded in the first place. Moreover, its policy should ensure that any protected health information recorded by the robots is secured and not shared with unauthorized parties.

Other federal agencies have jurisdiction to regulate or at least provide guidance about data protection practices for advanced technologies used in other sectors. For instance

- The Food and Drug Administration provides guidance for premarket submissions for and post-market management of cybersecurity issues.[28]
- Public utilities commissions regulate privacy and security requirements for smart meters.

---

25. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).
26. The Health Information Technology for Economic and Clinical Health Act within the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).
27. For a discussion of the impact of HIPAA security requirements on the use of advanced technologies, including artificial intelligence, robotics, Big Data, and the Internet of Things, see Stephen S. Wu, *A Guide to HIPAA Security and the Law* 255-73 (2016).
28. U.S. Food and Drug Administration, *Cybersecurity* (last visited Mar. 11, 2019), https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm (web page with links to various guidance documents).

- The Department of Energy's programs promote security for Big Data from smart meters and sensors, as well as security requirements for critical power grid infrastructure and integrated distributed energy resources.
- The Federal Communications Commission and the Department of Transportation oversee Security protocols for connected vehicle communications.
- The Department of Defense provides cybersecurity guidance and policies that govern the procurement and operation of Internet of Things devices.

Aside from these sector-specific data protection laws, businesses selling or operating advanced technology systems also need to comply with general state breach notification and security laws. Beginning with California in 2003,[29] states began requiring that businesses holding various categories of unsecured personal information about state residents notify those residents of security breaches that compromise their personal information. All states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have breach notification laws. Personal information covered by breach notification laws include social security numbers, driver's license/state ID numbers, and financial account numbers in combination with a PIN, password, or other identifier facilitating use of or access to financial accounts.[30]

A number of states go further and require businesses to take reasonable measures to protect the security of personal information about state residents. A prime example is California's AB 1950.[31] A business subject to federal or state law providing greater protection for personal information, however, is deemed in compliance with AB 1950.[32] Other states have similar laws. Practitioners should also bear in mind the possible scope of federal preemption of these state laws, especially as Congress considers federal data protection and breach notification legislation.

Massachusetts, however, has a more detailed set of information security requirements. The Massachusetts Office of Consumer

29. Cal. Civil Code §§ 1729.29, 1798.82.
30. *See e.g.*, 815 ILCS §§ 530/1-530/25; N.Y. Bus. Law. § 899-aa; N.Y. State Tech. Law § 208.
31. Cal. Civil Code § 1798.81.5.
32. *Id.* § 1798.81.5(e)(5).

Affairs and Business Regulation issued regulations[33] in 2008 to implement the Massachusetts security breach and data destruction law.[34] Unlike the state security laws discussed in the previous paragraph, the Massachusetts regulations require a written information security program with specific security controls that businesses holding personal information about Massachusetts residents must implement.

Businesses using advanced technologies that receive, store, or transmit any of the covered data elements must comply with these state data protection and breach notification laws. Manufacturers selling or licensing these technologies will want to make sure their systems facilitate compliance by their customers. Customers may negotiate agreements with them that places the responsibilities for compliance violations and data breaches on them without constraints of the normal liability caps vendors place in agreements.

Likewise, businesses will need to account for the new California Consumer Privacy Act[35] (CCPA) when it goes into effect in 2020, as well as any other state laws that follow on CCPA. CCPA provides "consumers" (California residents) with certain individual rights, such as the right of disclosure about the collection, use, and disclosure of personal information, the right to demand erasure of personal information, and the right to opt out of the sale of personal information. Businesses collecting personal information in connection with the sale or operation of advanced technologies will need to comply with CCPA once it becomes effective.

Also, businesses should take into account laws against unfair and deceptive trade practices. Examples include the Federal Trade Commission Act Section 5,[36] California's Unfair Competition Law,[37] California's False Advertising Law,[38] and similar laws in other states. The Federal Trade Commission regularly brings enforcement actions against businesses failing to secure their advanced technology products. Manufacturers and sellers that misrepresent their privacy or security practices or fail to include reasonable security features in their products may face federal or state enforcement actions or private party class action suits.

33. 201 CMR §§ 17.00-17.05.
34. Mass. Gen. Laws Ch. 93H, § 2(a).
35. Cal. Civil Code §§ 1798.100-1798.198.
36. 15 U.S.C. § 45.
37. Cal. Bus. & Prof. Code § 17200.
38. Cal. Bus. & Prof. Code § 17500.

Finally, businesses may need to meet the requirements of GDPR and other foreign data protection laws. If they have customers from or operations in foreign countries or receive personal data from foreign countries, they should determine if they fall under these laws and how those laws affect them. More details about the requirements of GDPR and these foreign laws appear elsewhere in this publication.

D. Process of Implementing an Effective Security and Privacy Program

There is no one single set of best practices when it comes to managing data protection programs. I have summarized and consolidated the management guidance in this section from a number of privacy and security management frameworks, including the Generally Accepted Privacy Principles,[39] materials from the International Association of Privacy Professionals,[40] and the Cybersecurity Framework of the National Institute of Standards and Technology.[41] I suggest reviewing these frameworks over time to supplement what appears in the six steps described in this section.

Step 1: A data protection program begins with aligning the business's overall strategy with its data protection strategy. With the business's culture in mind, this step involves planning the strategic direction and commitment of the business to data protection. The business will need to understand critical business requirements and imperatives that affect the program. Also, are there opportunities that dovetail with the business's strategy, such as positioning in the marketplace as a leader in data protection as part of an overall marketing strategy? Finally, the business will need to allocate sufficient resources for the program. The businesses should craft this strategy with the features, capabilities, and vulnerabilities associated with advanced technologies.

Step 2: The business will need to understand its current data protection posture. Most fundamentally, it will need to know what kind of personal data it is collecting and the flow of personal data throughout its systems during the entire data lifecycle from collection

39. American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants, Generally Accepted Privacy Principles (Aug. 2009).
40. International Association of Privacy Professionals, Privacy Program Management: Tools for Managing Privacy Within Your Organization (2013).
41. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2 (Dec. 5, 2017).

or generation to disposal or long-term archiving. It will need an understanding of all the information assets (its, customers, and vendors' networks, sets of servers, workstations, mobile devices, and storage systems) within the scope of the program. The business will need to understand the applicable laws creating data protection compliance requirements, contractual requirements, and industry requirements such as the Payment Card Industry Data Security Standard. Moreover, the business should conduct and update a risk assessment of the universe of potential data protection threats associated with advanced technologies, the likelihood and frequency of these threats coming to pass, the impact of the harm from these threats, and the controls available to mitigate these threats or their impact. The business's risk management process should prioritize a set of controls to mitigate the threats analyzed. Inevitably, the business will identify gaps between its current data protection posture and its target (ideal) profile of its organization. The business will need to prioritize the identified gaps and develop an action plan to address these gaps.

Step 3: This step consists of implementation of the program of controls developed in the previous step. For instance, the business should implement its action plan to begin closing gaps in its data protection program as it relates to advanced technologies. The business may assign people to implement specific programs to improve its data protection posture. In addition, this implementation phase involves ongoing data protection support of day-to-day business line operations. For example, data protection attorneys may be involved in regular negotiations of customer and vendor contracts or mergers and acquisition activities, including the due diligence involved in these transactions. They may also work with cross-functional teams to support new infrastructure, products, and services relating to advanced technologies. They may be involved in advising clients on data protection issues that come up in operations, such as questions about implementing data protection instructions or advising marketing professionals about data protection in connection with advertising campaigns. Data protection attorneys may provide advice about specific customer or employee situations that arise. Litigation data protection counsel may be involved in defensive or offensive claims relating to breaches, defects in products or services, or defaults in product or service agreements.

Step 4: Businesses should take steps to sustain and manage their data protection programs. They will need to monitor and provide day-to-day oversight over the implementation of the program to detect

issues and violations, and report and respond to them. A key part of the oversight function is providing training of personnel to make sure they understand their data protection functions. Moreover, data protection attorneys should facilitate the process of holding personnel accountable for compliance with the program. For instance, they may promote the use of data protection goals and objectives during employment reviews and advise internal clients concerning disciplinary actions taken following violations.

Step 5: Businesses should have formal programs of assessment and auditing of their data protection practices covering advanced technologies. Data protection attorneys may work together with internal and external auditors to assess and audit privacy and security compliance. Periodic audits may occur in connection with internal audits and external audits for privacy and security attestations or certifications, such as SOC reports on security or privacy or ISO 27001 security certifications.

Step 6: Businesses should periodically evaluate their data protection practices and make adjustments to their data protection programs. They may need to make changes because of information gleaned from data protection assessments, for instance to upgrade certain aspects of the program, undertake new privacy programs, or acquire new security tools. Businesses may need to integrate changes to applicable law or industry practice into their compliance programs and data protection controls. Changes in business models, advanced technology capabilities or vulnerabilities, or security threats may call for other changes.

Data protection attorneys play a vital role in overseeing these six steps. They can provide advice and counsel to data protection professionals and lines of business. Finally, they can report on the data protection program to upper management and boards.

III. PRIVACY ISSUES RAISED BY ADVANCED TECHNOLOGIES

Privacy risks from artificial intelligence, robotics, Big Data, and the Internet of Things stem from eight main causes: (1) the unwanted, surprising, intrusive, and/or opaque collection of more varieties of personal data than ever before; (2) the volume of personal data collected giving data controllers more capabilities; (3) the velocity of collecting, using, and sharing personal data giving data controllers more abilities to act on that personal data; (4) issues with the veracity of personal data; (5) bridging contexts, allowing data controllers to use personal data from disparate sources to profile data subjects; (6) surveillance capabilities in physical and virtual

spaces previously outside the capabilities of data controllers; (7) the lack of control over personal data; and (8) the direction of marketing messages to data subjects in new and unanticipated ways. This section discusses each of these issues in turn. The last subsection discusses blockchain privacy issues.

As mentioned above, sometimes the synergies among these technologies give rise to privacy issues. Big Data collected by Internet of Things sensors allow data controllers to use analytics and machine learning/artificial intelligence to analyze the data and take actions regarding a data subject. Those IoT sensors may be in or on robots or automated vehicles. In these cases, it is the combination of advanced technologies used that raise the privacy issues discussed in this section.

A. Greater Varieties of Personal Data Collected, Used, and Shared

New technologies make it possible for data controllers to collect a much larger variety of personal data than ever before. IoT devices collecting personal data range from the small scale – for instance, devices (eventually at nano scale) ingested, injected, or embedded in the human body – to the worldwide views possible with services like Google Earth, as well as the myriad of devices at scales anywhere between these extremes. We may give informed consent to allow devices into our body during surgical procedures, but Google collects data about our homes and streets (for Street View) without notifying us or allowing us to consent.

Businesses may minimize legal risk by providing additional notices, including location- and time-specific notifications. For instance, a building owner can mitigate the risk of invasion of privacy suits regarding IoT video cameras by being selective about the location of these cameras (e.g., avoiding sensitive locations) and posting notices about video recording in the public spaces where cameras are placed. Employers can disclose to workers in employment manuals that they are using security cameras in non-sensitive areas of the office.

Businesses collecting clickstream data or mobile device data in privacy policies. Nonetheless, few consumers read privacy policies. Accordingly, educating users about privacy controls and showing consumers privacy notifications immediately before a new personal data collection process would mitigate legal risk.

B. Greater Volume of Personal Data

To some extent, the sheer volume of personal data collected creates its own set of privacy issues. For instance, one mobile purchase in isolation might not mean very much. Nonetheless, collecting entire purchase histories of a user and the user's household would give a merchant and much clearer picture of purchasing interests and allow it to direct more targeted advertising to that household's members. The greater volumes of Big Data collected increase the possibility of leakage and inadvertent disclosure, even aside from the greater security risks. Moreover, large volumes of personal data about an individual in one context may make it more likely that de-identified data about that individual can be re-identified.

Businesses collecting, using, and disclosing large volumes of personal data should use controls with rigor commensurate with the volume of data collected to manage the collection, use, and disclosure of personal data. Greater transparency about the types and sources of data collected will promote trust in the data controller. Minimizing the volume of personal data collected or using de-identification will likely reduce legal risks associated with personal data volume.

C. Greater Velocity of Personal Data

The rapid analysis of Big Data (perhaps through machine learning) may make immediate action possible for a data controller in ways not possible in previous eras. For instance, consider the combination of geolocation and purchasing data history in a retail scenario. Let's say that a shopper has an app on his or her phone that communicates with a smart retail kiosk in a mall. When the shopper first walks into the mall, the hallway kiosk detects the shopper entering and performs a lookup. The mall's retail system can review the shopper's purchasing history and serve up a targeted display ad on the kiosk reflecting a special ad or discount offer based on the shopper's interest. The ad appears almost instantly as the shopper approaches and is about to pass by. The speed with which data can be collected and turned into action is increasing.

Again, a business using such a system can clearly explain the way it collects data, how it uses that data, and how it impacts the consumer. Since consumers don't read privacy policies, it would reduce privacy risks by providing context-specific notifications and opt-out options. Imagine a shopper that has been looking for an engagement ring to surprise his or her partner. In the absence of a control, the mall kiosk

we are discussing might display engagement ring ads as the shopper walks in the door. Now, imagine that the shopper brings his or her partner to the mall. That shopper would likely want to opt out of targeted ads right before entering the mall with his or her partner to avoid the possibility of seeing engagement ring ads that would spoil the surprise. Offering an easy way to opt out in specific contexts would help give the shopper control over the experience.

D. Issues of Veracity of Personal Data

With Big Data, questions arise concerning the veracity of personal data. Biased or incorrect data may lead to incorrect results of automated data processing. Intentional or unintentional corruption of data may also cause mistakes.

As mentioned in Section II.C.1, the EU's General Data Protection Regulation provides data subjects with the rights to an explanation and human intervention when automated data processing using personal data affect a data subject. These rights help correct mistakes caused by bias, incorrect data, or corruption of data. These GDPR rights are mandatory for GDPR-covered businesses. Nonetheless, using such techniques will also minimize legal risks for businesses outside the scope of GDPR.

E. Issues with Bridging Contexts of Personal Data Collection and Use

In our era of Big Data collection, cloud computing, and interoperability, it is increasingly common for businesses to collect data sets from different sources and combine or compare them to create more comprehensive profiles of data subjects. Data subjects that consent to data collection in disparate contexts may be surprised to find out that the collecting businesses have combined data sets to see new patterns and correlations.

Businesses can use greater transparency in their notifications to explain the sources of personal data they rely upon and how they use different data sources. Forthright disclosures can diffuse data subjects' surprise. Moreover, just-in-time and context-specific disclosures can provide additional notifications to data subjects, thereby reducing legal risk.

F. Greater Surveillance Capabilities

New IoT devices are observing data subjects in ways not possible in previous generations. Smart speakers and Siri chatbots are listening and, when triggered, record voice data. IoT cameras record video in increasingly large areas of public spaces, as well as workplaces, entertainment locations, businesses, and homes. People are concerned that drones flying near our homes are recording private activities. Pervasive surveillance is shrinking the areas in which we used to feel free from intrusion.

Currently, affective computing systems are trying to watch individuals to determine their emotional states and act accordingly. At some point in the future, AI systems fed by IoT data may be able to read minds. We have always thought that the last bastion of privacy was our internal thoughts in our minds. When the day comes that AI systems can read minds, even that last bastion will fall. This prospect is a scary one indeed. Fortunately, that day is not near, but we should at least monitor developments in AI to remain vigilant about the privacy of our mental states and thoughts.

In today's world, private businesses can minimize legal risk by providing location-specific notifications of data recording. Businesses providing smart speakers can provide clear disclosures of when voice recording occurs, what voice data is captured, and how long it is retained. Commentators have also talked about requiring device-specific interface mechanisms to warn people of data collection. For instance, drones with cameras could turn on a red light to warn people that video recording is taking place. Legislation may be necessary when market solutions fail to address specific privacy threats.

G. Lack of Control Over Personal Data

Some privacy complaints stem from a lack of control. A prime example is the data collection, use, and disclosure practice of credit bureaus. Unless consumers use identity theft services of a credit bureau, a consumer has no direct contractual relationship with credit bureaus that have a critical role in lending decisions about the consumer. Federal statutes give consumers limited rights to correct information.

In the IoT context, a data subject may have no way of receiving notice of or opting out of personal data collection. Imagine a guest in the home of a consumer who bought a smart speaker, or a child talking into a playmate's toy that collects voice data. The guest and the child in these examples have no relationship with the company selling

the device. They are simply bystanders whose data is collected. And as non-purchasers, they may have no rights under consumer protection laws to access collected data or insist on erasure.

It may be that in today's life, people should be educated about greater data collection possibilities and simply exercise caution about what they say in areas in which they have no control. And it may be that legislation will become necessary to curb abuses. In the meantime, privacy notices can raise the issue of bystanders and educate consumers about respect for the privacy of their friends and family members. In addition, interface mechanisms can promote transparency. For instance, smart speakers that light up when recording or toys that display a signal when recording is occurring can promote transparency to bystanders.

H. New Ways to Direct Marketing Messages to Data Subjects

Advertisers are always looking at new ways to target ads to consumers. Section III.C talks about smart kiosks in malls directing targeted ads to shoppers. We may expect retail environments to target us. But there may be new and innovative ways to deliver ads in ways impossible in previous years. For instance, imagine that you are instructing your automated vehicle to drive to a business establishment from the airport. That automated vehicle may calculate your route and notify you that a location of your favorite coffee shop is on the way to your destination and may ask if you want to stop there for refreshment, perhaps coupled with a special discount offer. More immediately, imagine that your smart refrigerator starts delivering discount coupons to its display. Previous generations of refrigerators have never delivered ads to their owners.

If current trajectories hold, it may simply be another fact of life that we are going to face more targeted advertisements in previously ad-free locations and contexts. Manufacturers and service providers can mitigate legal risks by notifying consumers about when they may deliver ads and offer them the ability to opt out. For instance, some presumably large swath of the population may never want to see ads coming from a refrigerator, even if purchasers could save money.

I. Blockchain and Privacy

One privacy issue that creates an interesting dilemma is the effect of the European Union's General Data Protection Regulation (GDPR)

and the California Consumer Privacy Act (CCPA) on blockchain technology. Blockchain technology used for public networks has inherent tensions with GDPR in that any personal data recorded on the blockchain is shared publicly.[42] Moreover, blockchain networks in which personal data is recorded can't delete records without breaking the blockchain, while GDPR would (in the absence of an applicable exception) require the erasure of personal data upon the data subject's demand.[43] The California Consumer Privacy Act would raise the same issue. The EU wrote a helpful summary of the effect of GDPR on blockchain technology with suggestions for mechanisms and controls to try to resolve these dilemmas.[44] Examples include:

- Questioning whether a blockchain is needed at all for specific applications.
- Avoiding the storage of personal data on the blockchain, and instead using mechanisms to minimize personal data collection and use, such as blockchains storing only pointers to off-blockchain data, obfuscating personal data, or encrypting personal data (coupled with cryptographic key destruction upon an erasure request).
- Using private blockchain networks with access controls, rather than public networks.
- Developing technological solutions to allow the erasure of blockchain data without breaking the blockchain's protections.[45]

IV. SECURITY ISSUES RAISED BY ADVANCED TECHNOLOGIES

IoT devices create a number of security threats. Consider the following threats, which would be shared by any computing system:

- Access to the device by unauthorized personnel.
- Weak authentication mechanisms (such as passwords).
- Lack of training leading to misuse or personal data leakage.

---

42. *See* The European Union Blockchain Observatory and Forum, Blockchain and the GDPR 16 (1st ed. 2018) (public blockchains are extremely distributed and GDPR compliance is easier if access is controlled to the blockchain), *available at* https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.
43. *See id.* at 25.
44. *See id.*
45. *Id.* at 25, 28-31.

- Weak physical protections allowing unauthorized personnel to access it, tamper with it, steal personal data from it, and/or inject malware into it.
- Weak transmission security, allowing attackers to intercept personal data.
- Malware compromising its functionality and/or compromising personal data.
- Network intrusion for purposes of stealing personal data and/or disrupting functionality.

The good news is that the expense of expensive robots and other sophisticated devices means that businesses will see a business case in spending time, attention, and resources protecting such devices with administrative, physical, and technical safeguards to address these threats. For instance, the expense of such devices makes it worth constantly updating device software and firmware during their lifecycle. Moreover, onboard processing resources coupled with external resources can facilitate diagnostic checks, security features, and alerts in the event of anomalous behavior.

By contrast, consider cheap, almost disposable sensors and other IoT devices. The security challenges with these devices are more acute because the it may not be worth the expense to monitor, maintain, and upgrade these devices. Consider the following threats to inexpensive IoT devices:

- They may have few processing, power, storage, and other resources to allow for diagnostic checks, security features, and alerting functions.
- It may be difficult, if not impossible, to update the software or firmware on the device with security patches.
- Cheap devices may not encrypt communications.
- Manufacturers may not have used secure software development practices.

For such devices, it may be that a number of controls may mitigate risk. Examples include:

- Embedding cryptographic key pairs into devices to facilitate encrypted communications with other computers.
- Using processors that save power, thereby increasing the ability of the device to conduct other security-related operations.

- Using secure software development to minimize vulnerabilities and focusing on top known code vulnerabilities.
- Enforcing (and notifying consumers of) expiration dates to make sure that devices that cannot be patched are taken out of service after a certain point in time.
- For devices that can be updated, making software patch updates transparent to users to prevent users from obstructing the patching process.

All IoT devices may face vulnerabilities such as:

- Default passwords that attackers may be able to discover, in situations where operators may not change default passwords.
- Hard-coded passwords vulnerable to discovery by attackers.
- Cryptographic keys stored in plaintext.
- Lack of enforcement of authentication protocols.
- Exploitable software vulnerabilities.

For instance, security researcher Billy Rios find these issues with the Hospira network-connected infusion pump.[46] An attacker compromising a device like an infusion pump could cut off medication flowing into a patient or cause the pump to multiply the dosage to patients. In either case, tampering could cause injury or death to patients. The above vulnerabilities violate basic security design principles and just applying basic principles can prevent these vulnerabilities.

Big Data and artificial intelligence systems for data analysis frequently run on enterprise software or, with increasing frequency, as software as a service applications. Software as a service applications create risk to businesses because they run on the vendor's servers and are beyond the business's direct control. Moreover, vendors commonly use cloud service providers to host the servers delivering the application such as Amazon Web Services, Microsoft Azure, or Google Cloud. Cloud service provider subcontractors further weaken control.

Mitigating risk requires due diligence on the vendor and any cloud service provider supporting the vendor's services. Customers are frequently demanding to view security audit reports and certifications of

46. Iain Thomson, *This hospital drug pump can be hacked over a network – and the US FDA is freaking out*, The Register, Aug. 1, 2015, https://www.theregister.co.uk/2015/08/01/fda_hospitals_hospira_pump_hacks/.

vendors and the cloud service providers as a part of due diligence and on an ongoing basis during performance of a service agreement. They may impose a series of requirements by security exhibits in service agreements. Where the SaaS services store personal data, customers also include privacy requirements in a privacy exhibit.

Blockchains face vulnerabilities that all cryptographic systems share, as well as vulnerabilities stemming from system architecture. A thorough discussion of blockchain vulnerabilities would be highly technical and beyond the scope of this chapter, but a few examples may suffice:

- Exploiting weakness in encryption algorithms and hash functions.
- Denial of service attacks.
- Manipulation of control in the system to create false transactions.
- Social engineering and man-in-the-middle attacks to compromise account information for wallets that can be exploited to drain wallets of value.
- Cryptojacking malware that causes infected machines to mine Bitcoin and other cryptocurrencies.
- Brute force attacks against cryptographic keys.

Risk mitigation techniques to ensure system integrity and protect the systems of Blockchain participants will require some combination of administrative, physical, and technical safeguards. Some Blockchain system architectures may face inherent security vulnerabilities and the best way to avoid risk in the short run is to use a different system that doesn't share these vulnerabilities. Users should protect their account credentials (e.g., passwords) and educate themselves about phishing and other schemes seeking to fool them into disclosing their account credentials. Malware detection software can now detect cryptojacking malware and businesses should scan their systems for this and other kinds of malware.

V. CONCLUSIONS

Artificial intelligence, robotics, Internet of Things, Big Data, and blockchain systems pose significant legal challenges. Their use may threaten the privacy and security of personal data. Businesses manufacturing, selling, purchasing, and operating these advanced technology systems may collect vast volumes of data of different varieties at increasingly greater velocities, while at the same time making data subject to bias, mistakes, and corruption. Increasing correlation of personal data among disparate

data sets, increased surveillance capabilities, and new ways of directing marketing messages to individuals intrude on privacy, while at the same time individuals' control over personal data is eroding. Internet of Things devices, including robots, may contain software vulnerabilities and their configuration may open them to hacking attacks. At the same time, cheaper IoT devices may not use safeguards such as encryption and may be impossible to update with software or firmware patches.

Nonetheless, businesses can mitigate privacy risks by enhancing their privacy practices and controls. Examples include enhanced transparent notices specific to context and location, de-identification of data and data minimization to minimize volumes of personal data at risk, enhancing opt-out mechanisms, offering procedures for humans to check the results of explainable automated data processing, using technical and interface methods to make data collection practices more transparent, and offering enhanced privacy controls. Businesses can secure devices and systems using these advanced technologies by implementing and maintaining administrative, physical, and technical security controls. Blockchain systems raise specific privacy issues by making erasure personal data in blockchain ledgers difficult, if not impossible, while their architectures open them up to attacks.

Advanced technologies are coming. They will have profound effects on society, both positive and negative. As a result, they will generate momentous legal issues, including in the areas of privacy and security. It will be up to lawyers to lead the way to use some of the safeguards discussed in this chapter to make sure clients' interests are protected, privacy and security are maintained, and businesses deploy advanced technologies in a safe, ethical, and compliant fashion.

NOTES

35

Blockchain: Challenges and Solutions for Compliance with the GDPR

Lydia de la Torre
Santa Clara Law School

Blockchain is a technology with a high potential for development that covers a very broad range of situations. Blockchains can serve to transfer assets (e.g.: Bitcoin or property deeds), be used as a ledger ensuring traceability (e.g.: diploma certification) or even to launch a smart contract (an independent programme that "freezes" an agreement reached by two people in a blockchain in the form of an algorithm).

When blockchain entails the processing of personal data, it raises legal compliance questions. For example, aligning the immutability of blockchain with the principle of storage limitation can be challenging. At the same time, blockchains can provide effective solutions to meet the requirements imposed by GDPR. For example, the immutability of actions carried out on blockchains can enable solutions that effectively trace consent.

This article discusses the responsible use of blockchain in the context of personal data and addresses the legal compliance questions of blockchain in the context of EU data protection law.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data (GDPR) is one of the three main data protection laws of the EU. The other two are the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of crimes offences or the execution of criminal penalties, and on the free movement of such dta (Directive 2016/680) and Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (Regulation 2018/1725). Because Directive 2016/680 and Regulation 2018/1725 do not apply to the private sector they will not be discussed in this paper.

GDPR represents an evolution rather than a revolution in the field of data protection law. The structure of EU data protection law represented in the GDPR was developed in the 80s and 90s at a time where centralized processing of data was the norm. The decentralized data government model used by blockchain technology results in a multitude of actors involved in the processing. This adds a layer of complexity to compliance with a legal framework that was not designed with blockchain in mind.

The analysis in this article draws heavily from the initial assessment on compatibility of blockchain and GDPR issued by the Commission Nationale de l'Informatique et des Libertés (CNIL) issued on November 6,

2018 and available at https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data but it also incorporates the author's perspective and analysis.

WHAT IS BLOCKCHAIN?

A blockchain is a **database** that stores data and that is distributed to a large number of computers. All entries, called "transactions", are **visible to all users**. Blockchains are defined by the following properties:

- **transparency**: all participants can view all data recorded;
- **sharing and decentralisation**: several copies of the blockchain coexist on different computers;
- **irreversibility**: once data is recorded, it cannot be altered or removed; and
- **disintermediation**: all decisions are made by consensus between the participants, without a central arbitrator.

The term "blockchain" is often associated with another term that refers to a larger family of technologies: DLTs, or "Distributed Ledger Technology". This article centers specifically on blockchain technology.

There are several types of blockchains, which use different permission levels for different categories of participants. This articles uses the following classification:

- **Public blockchains** are accessible to all, anywhere in the world. Anyone can record a transaction, take part in the validation of the blocks or access a copy of them;
- **Permissioned blockchains** have rules that set out who can take part in the validation process or even register transactions. They can, depending on the case, be accessible to all or be restricted;
- **"Private" blockchains** are controlled by a unique actor who alone oversees participation and validation.

Because 'private' blockchains do not include the traditional properties of blockchains (such as decentralisation and shared validation) they do not raise the same compliance issues raised by non-private blockchain. GDPR compliance for private blockchain is less demanding and will not be discussed in this article.

This article distinguishes between three types of blockchain actors:

- **"accessors"**, who have the right to read and hold a copy of the chain;
- **"participants"** who have the right to make entries (i.e., make a transaction for which they request validation);
- **"miners"** who validate a transaction and create blocks by applying blockchain rules for "acceptance" by the community.

A blockchain can contain two categories of personal data:

- **participants' and miners' identifiers**: each participant/miner has a public key, ensuring identification of the issuer and receiver of a transaction;
- **additional data** contained "within" a transaction (e.g.: diploma, property deed). If this data concerns natural persons, possibly other than the participants, who may be directly or indirectly identified, such data is considered personal data.

BLOCKCHAIN AND GDPR COMPLIANCE

As part of its Data Protection by Design obligations (Article 25 GDPR), the data controller must give prior thought to the appropriateness of choosing this technology to implement its processing. Blockchain is not necessarily the most suitable technology for all data processing and it can be a source of difficulties for data controllers in terms of compliance with the obligations set out by the GDPR.

This section analyses blockchain technologies in the light of the scope of GDPR, its data protection principles, the identification of controllers and lawful basis, the data subject rights under GDPR, the obligations of controllers and processors, the issues related to transfers outside of the EU and security. It provides provides advice on best practices for blockchain participants based on the analysis which are summarized below

Summary of advice on best practices for blockchain participants

1. Unless the 'purely personal or household activity' exemption applies**, the processing of personal data by blockchains is subject to GDPR**.
2. Participants should **carefully select the type of blockchain** that aligns with their design to the data protection processing principles

under GDPR (in particular, the principle of storage limitation) and, to the extent possible, minimize the personal data stored in the chain

3. **No existing technical solutions can guarantee compliance with the principle of storage limitation** under GDPR as it is currently interpreted. As a matter of best practice, storage of personal data outside of the blockchain is recommended.
4. In a blockchain, (i) **participants** with the right to make entries **act as a data controllers**; (ii) **miners** (who validate the transaction containing personal data on a blockchain) **act as processors**; and (iii) **accessors may be acting either as processors or controllers** if the 'purely personal or household activity' exemption does not apply.
5. When a **group of participants** decides to carry out processing operations on a blockchain for a common purpose they will, by default, be considered joint controllers under GDPR. Given the complexities that this would create it is advisable for participants to create a legal person to be the data controller or designate a participant to make decisions for the group.
6. The **smart contract developer** who processes personal data on behalf of the participant, who is the data controller; can act as a processor.
7. Blockchain participants must **carefully identify the lawful basis** for processing and keep in mind their correlation to data subject rights.
8. The rights of information, of access and of portability are not, at first glance, particularly problematic on the blockchain technology **implementing the right to erase, the right to object, and the right rectify can be challenging** but there are technical solutions for the exercise of those rights that can move closer towards a compliance with the GDPR**.**
9. The requirement for appropriate safeguards for **transfers outside the EU**, such as binding corporate rules or standard contractual clauses, are entirely applicable to permissioned blockchains. For GDPR compliance purposes, permissioned blockchains should be favoured as they allow a better control over personal data governance, in particular as regards transfers outside of the EU.

10. Overall the security of blockchain technology is robust but not infallible. Participants should carefully design the blockchain to minimize potential security issues.

TERRITORIAL AND MATERIAL SCOPE

GDPR applies to actors that participate in a blockchain provided that they (1) have an 'establishment' in the EU and process data 'in the context of the activities of the establishment' or (2) offer goods or services targeted to EU residents (Article 2 & 3 of GDPR). Therefore, it is possible for some but not all blockchain actors to fall within the scope of GDPR. Given the fact that controller liability is, by default, joint and several (see Article 26 of GDPR) where any of the participants in a blockchain are 'established' in the EU or the services of the blockchain are to be offered to EU residents, it would be advisable to ensure that the whole blockchain is compliant with GDPR.

Activities that are performed by a natural persona and are **"purely personal or household"** in nature are excluded from applicability of GDPR (see Article 2.2.(c)). Therefore, as a general rule, the activities of any natural person that processes personal data on the blockchain are not subject to GDPR if those activities do not relate to a professional or commercial activity pursuant to the **"purely personal or household activity"** exclusion. For example, a natural person who buys or sells Bitcoin, on his or her own behalf, is not subject to GDPR. However, the said person can be considered a data controller if those transactions are carried out as part of a professional or commercial activity, or on behalf of other natural persons.

PRINCIPLES

There are seven principles that any entity must abide by while processing personal data subject to GDPR (see Article 5 of GDPR). From the seven principles there is one that arguably directly conflicts with blockchain technology: The principle of storage limitation

The principle of storage limitation stands for the proposition that personal data cannot be stored for an unlimited time. A data retention period must therefore be defined according to the purpose of the data processing. However, one of the characteristics of blockchains is that the data registered on a blockchain cannot be altered or deleted: once a majority of participants accept a block in which a transaction is recorded, that transaction can no longer be altered in practice.

As a reminder, a blockchain can contain two categories of personal data:

- **The identifiers of participants and miners**: Each participant has an identifier comprised of a series of alphanumeric characters which appear random and constitute the public key to the participant's account. This public key is linked to a private key known only by the participant.
- **Additional data (or payload)**: Besides the participants' identifiers, the additional data stored on the blockchain can contain personal data that can potentially relate to individuals other than participants and miners.

GDPR requires data controllers to choose the format with the least impact on individuals rights and freedoms (under data protection by design set out in Article 25 of the GDPR).

Some technical solutions have been examined by stakeholders in order to solve this issue and are described below. However their **ability to ensure full compliance with the GDPR is questionable**.

Some data controllers may have a **legal obligation to publicize some information** and make it accessible, without a retention period: in this particular case, storage of personal data on a public blockchain can be envisaged (see, "Lawful basis" section below). In addition, if justified by the purpose of the processing and if a **data protection impact assessment (DPIA)** proves that the residual risks are acceptable, personal data may be stored on the blockchain, in the form of a traditional fingerprint (without a key) or even in cleartext.

As a matter of best practice:

- With respect to the **identifiers of participants and miners** (i.e. their public keys), blockchain architecture means that these identifiers are inherently always visible, as they are essential for its proper functioning. Because miners and participant identifiers in blockchain cannot be stored off the chain or further minimised, the retention periods are de-facto equal to the duration of the blockchain itself as they are essential for proper functioning. Given that it is not possible to further minimise the identifiers, no additional steps can be taken to ensure compliance.
- With respect to **payload data**, implementing solutions that enable **storage of the data outside of the blockchain is recommended**. The common feature underlying some of these solutions is to store any data in cleartext outside of the blockchain (for example, on the

data controller's information system) and to store on the blockchain only proof of existence of the data (e.g. commitment, hash generated from a keyed hash function, etc.).

- Where storage of payload data outside of the blockchain is not feasible, data could be stored either using a hash function without a key or, in the absence of any other possibilities, in cleartext but only when justified by the purpose of the processing and where a DPIA has proven that the residual risks are acceptable.

Where storage of personal data must occur, registering personal data on the blockchain in the **form of a 'commitment' is preferable** for GDPR compliance (a "commitment" is a cryptographic mechanism that allows one to "freeze" data in such a way that it is both possible - with additional information - to prove what has been frozen and impossible to find or recognise such data by using this sole "commit"). Where this is not feasible, registering the data in the form of a hash generated using a hash function with a key would be the best alternative. Where that is not a viable option, data should at least be registered in the form of an encryption ensuring a high level of confidentiality (a ciphertext).

CONTROLLERS AND PROCESSORS IN A BLOCKCHAIN

The first step to identify GDPR obligations is to **identify the role that the different blockchain actors take with respect to the processing**. Determining who acts as the controller is a key exercise, since data subjects (i.e. those whose personal data is recorded on the blockchain) must be informed about which entity they can refer to in order to effectively exercise their rights, and data protection authorities must have a contact point who can be held accountable for the processing carried out.

Under GDPR, entities processing personal data are either controllers or processor. These roles were designed in a time where data management was centralized within specific technologies. As a general rule, **an entity acts as a controller if it defies the means and purposes of the processing** of personal data while an entity acts as a **processor when it is processing data on behalf of a controller** s (see Article 4 (7)&(8) of GDPR). The test to determine who acts as a controller is factual based: any entity that de facto determines the means and purposes of processing takes the role of controller under GDPR. It is also specific to the processing performed: an entity may act as a controller as to a specific process related to a specific personal data set and simultaneously as a processor regarding a different process related to the same personal data set.

In the context of blockchain:

- **Accessors** (i.e. persons with the right to read and hold a copy of the chain): Because processing is defined under GDPR to include access (see Article 4(2) of GDPR), assessors who access data of individuals other than themselves process data under GDPR unless the "purely personal or household" exemption applies. They may be acting either as processors (if they access on behalf of someone else) or as controllers. This classification gives rise to significant practical compliance challenges.
- **Participants** (i.e. persons deciding to register data on a blockchain): Because participants determine the means and purposes of the processing they are considered **data controllers.** Where participants have the right to write on the chain, and are able to decide to send data for validation by the miners, they can be considered as data controllers since they define the 'purposes' (objectives pursued by the processing) and the 'means' (data format, use of blockchain technology, etc.) of the processing. By default, they will be considered joint controllers, required to document their relationship (see, Article 26 of GDPR). For example, if a notary records his or her client's property deed on a blockchain, the said notary is a data controller. In addition, if a bank enters its clients' data onto a blockchain as part of its client management processing, it is a data controller.
- **Miners**: Because miners only validate transactions submitted by participants and are not involved in the object of these transactions, they do not define the purposes and the means of the processing and, therefore, are not controllers. In some cases miners can be considered **data processors**, as they follow the data controllers' instructions when checking whether the transaction meets technical criteria (such as a format and a certain maximum size, and that the participant is allowed, according to the chain rules, to carry out its transaction). This classification gives rise to significant practical difficulties, especially for miners in a public blockchain.

Given the complexity this would create, it can be **useful to identify a data controller beforehand**. This can be done by creating a legal person in the form of an association or economic interest group or by identifying one participant who is responsible for making the decisions for the group and designating the said participant as a data controller. Such entity/participant could be considered the controller with the other participants acting as processors provided that the participants that act as processors

do not de-facto determine the "purposes and means" of the processing (in which case they will be de-facto controllers). Otherwise, all participants will likely be considered joint controllers subject to joint and several liability and required to determine, in a transparent way, their respective responsibilities to ensure compliance with GDPR (see Article 26 of GDPR).

Regarding **software developers for smart contracts solutions**, the algorithm developer may simply be a solution provider or, when the said algorithm developer participates in the processing, may be qualified as a data processor or data controller depending on its role in determining the purposes of the processing. For instance, a software developer offers a solution to an insurance company, in the form of a smart contract that enables passengers to be automatically reimbursed when their flight has been delayed. This developer would be qualified as a data processor if he or she intervenes in the processing of personal data, the insurance company being the data controller. The developer should therefore establish a contract with the participant, acting as data controller, specifying each party's obligations and ensure that the contract reproduces the provisions of Article 28 of the GDPR. On the other hand, if several insurance companies decide to create a permissioned blockchain for their processing operations, the purpose of which is compliance with their KYC ("Know Your Customer") obligations, they may decide that one of them is the data controller. In this case, the other insurance companies, which validate transactions as miners, are likely to be considered as data processors.

LAWFUL BASIS

The core requirement of EU data protection law since its inception has been that information technology should be **used only for purposes that benefit humanity**. In order to achieve this goal, **EU data protection law in general and GDPR in particular require that the purposes for every processing be identified and mandates that they must be legal**. In order to be legal, a purpose must fall within one of six categories of purposes or 'lawful basis' (see, GDPR Article 6).

Therefore, participants in a blockchain are required to identify and document the **lawful basis** for the processing of personal data. From the six existing lawful basis for processing the four that are most relevant to blockchain are contractual necessity, legitimate interest, public interest and legal obligation.

In practice, blockchains will rarely be able to rely exclusively on **'contractual necessity'** as a lawful basis. This is due the the fact that the use

of contractual necessity is only available where the processing is necessary to **fulfil contractual obligations between the controller and the data subject or because the data subject asked the controller to do something required before entering into a contract**. However, contractual necessity may be a viable option form performing some of the processing required for blockchain based smart contracts solutions.

Where the processing is carried out on the basis of **contractual necessity**:

- The specific data being processed should be limited to what is necessary to comply with a contract or enter into a contract. **'Necessary'** does not mean that processing must be essential for the purposes of performing a contract or taking relevant pre-contractual steps. However, it must be a targeted and proportionate way of achieving that purpose.
- The actual existence of an enforceable contract under the law is not required provided that the processing relates to a first step (e.g. provide a quote) and the processing is required for that purpose. Therefore, this lawful base does not apply where the controller takes pre-contractual steps on its own initiative or at the request of a third party.

Where the processing takes place on the basis of contractual necessity, **data subjects do not have a right to object** to the processing.

Legitimate interest is the most flexible lawful base under GDPR but is not always appropriate. A **wide range of interests may be legitimate interests** including the controller´s own interests or the interests of third parties. The processing must be **'necessary'** to accomplish the legitimate interest, meaning that the processing must be a targeted and proportionate way of achieving a purpose and that controllers cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

Controllers must balance their interests against the data subject's interests. In particular, if data subject's would not reasonably expect the processing, or it would cause them unwarranted harm, their interests are likely to override the interest of the controller. To rely on legitimate interests controllers must perform a balancing test. There's **no foolproof formula** for the outcome of the balancing test but the legal requirements to use legitimate interest as a lawful basis can be broken down into **three-parts**:

(1) **Purpose test**: are the participants pursuing a legitimate interest? To identify the legitimate interest participants in blockchain should

consider what the blockchain is trying to achieve including the potential benefits to the public and the relative importance of those benefits.

(2) **Necessity test**: is the processing necessary for that purpose? In order to assess the necessity participants in blockchain should consider if the blockchain actually helps advance the interest identified through the purposes test and if there are other less invasive ways to advance the same interest.

(3) **Balancing test**: does the data subject's interests override the legitimate interest? Blockchain participants must consider the impact of the processing and whether this overrides the interest identified. It can be helpful to consider the nature of the participant's relationship to the data subjects whose data is processed, the nature of the data itself, the expectations of the data subject, and the potential impact to the data subjects. Processing children's data should be weighed heavily in the balancing test.

When the processing is done under legitimate interest, data subjects **do not have the right to data portability**.

Where the processing is done on the basis of **public interest** no balancing test is required. However, public interest is only available where participants need to process the personal data 'in the exercise of official authority' (this covers public functions and powers that are set out in law); or to perform a specific task in the public interest that is set out in law. This lawful base can only be used for blockchain solutions deployed by EU or Member State public authorities or by participants who are performing an underlying task, function or power that has a clear basis in EU or Member State law (see, GDPR article 6.3).

Where the processing is on the basis of public interest, **the individual has no right to erasure, or right to data portability**.

Processing on the basis of **legal obligation** is only possible where controllers are required to process the personal data to comply with EU or Member State law (see, Article 6 (3) of GDPR)**.** Recital 41 of GDPR confirms that this does not have to be an explicit statutory obligation as long as the application of the law is foreseeable to those individuals subject to it, including clear common law obligations.

This lawful basis is available where the overall purpose of a blockchain is to comply with a legal obligation that has sufficiently clear basis in either EU law or Member State common law or statute. Blockchain participants **should be able to identify the obligation** in question, either by reference to the specific legal provision or by pointing to an appropriate source of advice or guidance that sets it out clearly (e.g. a government

website or industry guidance that explains generally applicable legal obligations).

Where the processing is on the basis of legal obligation, **the individual has no right to erasure, right to data portability, or right to object**.

Finally, because controllers that process **special categories of data** must identify a separate lawful base that applies to those categories of data (see Articles 9 and 10 of GDPR), it is advisable for blockchain technology to avoid processing special categories of data. This can make the use of blockchain in the healthcare sector particularly challenging.

DATA SUBJECT RIGHTS

The GDPR was designed to **give control back to individuals**. It strengthened individuals' rights against those who process their data and, in addition, created new rights.

Besides minimising risks to individuals, as mentioned above, the format chosen to register the data on a blockchain can also facilitate the exercise of individual rights.

Some rights are entirely compatible with a blockchain. For example, the right to be informed can be complied with by requiring the data controller to provide concise information that is easily accessible and formulated in clear terms before the data subject submits information. The same applies to the right of access or the right to portability.

Other rights present special challenges in the context of blockchain. In particular implementing the **right to erase, the right to object, and the right rectify** can be challenging but there are technical solutions for the exercise of those rights that can move closer towards a compliance with the GDPR.

Similar to risk minimization, the choice of a proper cryptological method to store the data allows the data subject to move closer to an effective exercise of his or her rights: erasure of data stored outside of the blockchain and of elements enabling their verification, which allow s for access to the proof recorded on the blockchain to be cut off, making and makes the data difficult and even impossible to retrieve. It is **technically impossible to grant the request for erasure** made by a data subject **when data is registered on a blockchain**. However, when the data recorded on the blockchain is a commitment, a hash generated by a keyed- hash function or a ciphertext obtained through "state of the art" algorithms and keys, the data controller can make the data practically inaccessible and therefore achieve the effects of data erasure.

The CNIL initial assessment on compatibility of blockchain and GDPR (issued November 6, 2018 and available at https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data) gives two examples of this:

- The mathematical properties of some commitment schemes can ensure that upon erasure of the elements enabling it to be verified, it will be no longer be possible to prove or verify which information has been committed. When a commitment scheme is perfectly hidden, deleting the witness (i.e. the element that allows to verify that a given value is committed in a given commit) and the value committed is sufficient to render the commitment anonymous in such a way that it can no longer be considered personal data. The commitment itself would therefore no longer represent any risk in terms of confidentiality. The information would also need to be deleted in other systems where it has been stored for processing.
- Deletion of the keyed hash functions secret key would have similar effects. Proving or verifying which information has been hashed would no longer be possible. In practice, the hash would no longer pose a confidentiality risk. Once again, the information would also need to be deleted in other systems where it has been stored for processing.

Excluding the specific case of some commitment schemes, **these solutions do not, strictly speaking, result in an erasure** of the data insofar as the data would still exist in the blockchain. However, the schemes allow data subjects to get closer to an effective exercise of the right of erasure.

It is technically impossible to grant the request for rectification or for erasure made by a data subject when cleartext or hashed data is recorded on a blockchain. It is therefore strongly recommended not to register personal data in cleartext on a blockchain.

With regards to the **right of rectification**, the impossibility to modify the data in a block must cause the data controller to enter the updated data in a new block. Indeed, a subsequent transaction can cancel an initial transaction even though the first transaction will still appear in the chain. The same solutions as those applied following a request for deletion of personal data could be applied to erroneous data when such data requires deletion.

A careful consideration in advance regarding the **right to restriction** (introduced by Article 18 of the GDPR) and to **human intervention** in the context of entirely automated decision-making (Article 22 Paragraph 3) is required. For example, it could be possible to **restrict the use of data**

in smart contracts simply by including this possibility in advance in the programme.

Exclusively automated decision arising from a smart contract is necessary for its performance, given that it enables the fulfilment of the very essence of the contract (i.e., the reason for which the parties concluded the contract). The data subject has a right to obtain human intervention, to express his or her point of view and to contest the decision after the smart contract has been performed. This basically requires the data controller in a smart contract solution to provide the possibility of human intervention (allowing the data subject to contest the decision even if the contract has already been performed, and regardless of what is registered on the blockchain).

CONTROLLER AND PROCESSOR OBLIGATIONS:

Complying with the **formal obligations of GDPR in term of record keeping and implementation of specific contractual provisions is a daunting task,** specially in the case of public blockchains where everyone can take part of the validation process. For example, controllers and processors are required to formalize relations through a written contract that must contain certain provisions (see, Article 28 of GDPR). On the other hand, joint controllers (see, Article 26 of GDPR) must determine their respective responsibilities for compliance with GDPR by means of 'an arrangement' between them (see Article 26 of GDPR). Both controllers and processors are required to keep records of processing activities (see Article 30 of GDPR).

In addition, controllers and processors need to consider their obligations to appoint a data protection officer, conduct data protection impact assessments, and implement data protection by design.

TRANSFERS OUTSIDE OF THE EU

Transfers outside of the European Union (EU) can be particularly problematic, especially in the case of public blockchains.

As a reminder, all transactions on the blockchain involve:

- a request to validate the transaction (and therefore potentially personal data) being sent to all miners of the chain;
- an update to the blockchain by adding a new block on the chain for all participants.

However, whether they are miners or not, participants can be located in countries outside of the EU. This therefore raises the question of compliance with obligations for transfers outside of the EU.

While appropriate safeguards for a transfer outside the EU may be used in a permissioned blockchain, such as standard contractual clauses, binding corporate rules, codes of conduct or even certification mechanisms, these safeguards are harder to implement in a public blockchain given that the data controller has no real control over the location of miners.

SECURITY

Regarding the security requirements, the different properties of a blockchain (transparency, decentralisation, tamper-proof and disintermediation) mainly rely on two factors: the number of participants and miners, and a set of cryptological mechanisms.

For permissioned blockchains, depending on the potential divergence or convergence of participating actors' interests, carrying out an evaluation of the minimal number of miners to prevent a coalition that could control over 50% of networking power over the chain is recommendable. To illustrate this point, recent cases show that a single entity or individual with greater than 50% of networking computer power can "rewrite the [blockchain] transaction history". https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

A majority of blockchain "hacks", however occur at the exchange level. Industry standard security practices can mitigate those threats. Therefore, it is important to set out technical and organisational security procedures to limit the impact of potential algorithm and security failures on transactions and exchanges, including an emergency plan enabling algorithms to be changed when a vulnerability is identified. An organization that implements a public blockchain should be particularly vigilant to newly identified threats in the context of smart-contracts, since source code is often publicly visible on the blockchain.

Governance of changes to the software used to create transactions and to mine should be documented, and technical and organisational procedures should be set out to ensure an alignment between planned permissions and practical application. If the blockchain is not public, the measures implemented to ensure confidentiality should be considered. Controllers carrying out processing through transactions on a blockchain should ensure the security of secret keys used, for example by ensuring that they are stored on secure media.

Overall the security of blockchain technology is robust. Organizations can maintain the integrity of a blockchain system by ensuring that the system is well executed from launch, proactively identify algorithm bugs, prevent single entity or organizations from amassing a majority of the network power control, and be aware of newly identified vulnerabilities. These processes, when carefully considered, documented and implemented, both ensure security and contribute toward a blockchain controller's compliance with the GDPR's legal obligations.

NOTES

NOTES

36

Wiley Rein Newsletter: Moving Toward a New Health Care Privacy Paradigm (November 2014)

Kirk J. Nahra

WilmerHale LLP (formerly with Wiley Rein LLP)

Moving Toward a New Health Care Privacy Paradigm

By Kirk J. Nahra

November 2014

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) has set the primary standard for the privacy of health care information in the United States since the rule went into effect in 2003. It is an important rule that creates significant baseline protections for health care information across the country.

Yet, from the beginning, the HIPAA Privacy Rule has had important gaps. The Privacy Rule was the result of a series of Congressional judgments about "scope"—driven by issues having nothing to do with privacy, like the "portability" of health insurance coverage and the transmission of standardized electronic transactions. As a result of the HIPAA statute, the U.S. Department of Health and Human Services (HHS) only had the authority to write a privacy rule focused on HIPAA "covered entities," meaning that certain segments of relevant industries that regularly use or create health care information—such as life insurers or workers compensation carriers—were not within the reach of the HIPAA rules. Therefore, the HIPAA Privacy Rule has always been a "limited scope" privacy rule, rather than a general medical privacy rule.

But, at least at the start, these gaps were somewhat limited, and large components of the health care industry—including most health care providers and health insurers—were covered by the HIPAA. What has changed in the past decade is the enormous range of entities that create, use and disclose health care information outside of the HIPAA privacy rule. We have reached (and passed) a tipping point on this issue, such that there is enormous concern about how this "non-HIPAA" health care data is being addressed, and how the privacy interests of individuals are being protected (if at all) for this "non-HIPAA" health care data.

So, what exactly is the problem and what is likely to happen to address it?

We have seen in recent years an explosion in the creation of "non-HIPAA" health care data. For example, numerous web sites gather and distribute health care information without the involvement of a covered entity (meaning that these web sites are not covered by the HIPAA Privacy Rule).

* * *

Kirk J. Nahra is a Partner with Wiley Rein LLP in Washington, D.C. He represents a wide variety of companies on privacy, data security, cyber-security, and security breach issues across the country and internationally. He chairs the firm's Privacy and Data Security practice. A long-time member of the Board of Directors of the International Association of Privacy Professionals and editor of IAPP's Privacy Advisor, he speaks and writes widely on a broad variety of privacy and data security issues. He can be reached at 202.719.7335 or knahra@wileyrein.com. Follow him on Twitter @kirkjnahrawork.

These range from commercial web sites (e.g., Web MD), to patient support groups, to the growth of personal health records. We also have seen a significant expansion of mobile applications directed to health care data or offered in connection with health information. Recent announcements from Apple and Google have expanded this large and growing area. Unless a covered entity is involved, these activities generally are outside of the scope of the HIPAA Privacy Rule, and are subject to few explicit privacy requirements (other than general principles such as the idea that you must follow what you say in a privacy notice).

This growth in "non-HIPAA" health care data is raising significant expressions of concern, by the FTC, privacy advocates and others, about how (if at all) this "non-HIPAA" health data is regulated and how the privacy interests of consumers are protected. As FTC Commissioner Julie Brill stated in a recent speech, "Big picture, consumer generated health information is proliferating, not just on the web but also through connected devices and the internet of things." As Ms. Brill indicated, this development involves "health data flows that are occurring outside of HIPAA and outside of any medical context, and therefore outside of any regulatory regime that focuses specifically on health information."

At the same time, we also have seen increasing discussion of the general concept of "Big Data" and the impact of "Big Data" on privacy and security.

While much of this discussion is outside of the context of health care, there is both a wide variety of health care information (HIPAA regulated and not) that is being scrutinized in the context of Big Data and a growing range of "Big Data" activities being conducted by health care entities, again both in and out of HIPAA.

In the context of this development, a recent White House report on Big Data stated that:

- A significant finding of this report is that big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace.

- The privacy frameworks that currently cover information now used in health may not be well suited to address these developments or facilitate the research that drives them.

- As big data enables ever more powerful discoveries, it will be important to re-visit how privacy is protected as information circulates among all the partners involved in care. Health care leaders have voiced the need for a broader trust framework to grant all health information, regardless of its source, some level of privacy protection.

- This may potentially involve crafting additional protections beyond those afforded in the Health Insurance Portability and Accountability Act and Genetic Information Non-Discrimination Act as well as streamlining data interoperability and compliance requirements.

Modernizing the health care data privacy framework will require careful negotiation between the many parties involved in delivering health care and insurance to Americans, but the potential economic and health benefits make it well worth the effort.

These developments have identified several significant concerns that are motivating this debate. First, much of the data that is being gathered is outside the scope of the HIPAA rules (and is therefore largely unregulated). The volume of this data is growing. Accordingly, there is a key issue as to how, if at all, this "non-HIPAA data" should be regulated.

Next, through the White House Big Data report, the FTC's Data Broker report and otherwise, substantial concerns have been raised about how this data is being used, in contexts that raise questions about how health care services are provided and appropriate rights and protections for individuals in connection with their health care and their privacy.

In addition, as "patient engagement" becomes an important theme of health care reform, there is increased concern about how patients view this use of data, and whether there are meaningful ways for patients to understand how their data is being used. The complexity of the regulatory structure (where protections depend on sources of data rather than "kind" of data), and the difficulty of determining data sources (which are often difficult, if not impossible, to determine), has led to an increased call for broader but simplified regulation of health care data overall. This likely will call into question the lines that were drawn by the HIPAA statute, and easily could lead to a re-evaluation of the overall HIPAA framework. In fact, this issue was raised specifically by Commissioner Brill in her recent speech, where she asked:

> then the question becomes, though, if we do have a law that protects health information but only in certain contexts, and then the same type of information or something very close to it is flowing outside of those silos that were created a long time ago, what does that mean? Are we comfortable with it? And should we be breaking down the legal silos to better protect that same health information when it is generated elsewhere.

At the same time, we also are seeing an increased usage by HIPAA covered entities of personal data that would not traditionally be viewed as "health care information." For example, a recent report published on Bloomberg.com discussed how physicians are obtaining a wide variety of behavioral indicators about their patients in order to monitor health risks. The story states that "You may soon get a call from your doctor if you've let your gym membership lapse, made a habit of picking up candy bars at the check-out counter or begin shopping at plus-sized stores." See Pettypiece and Robertson, "Your Doctor Knows You're Killing Yourself. The Data Brokers Told Her," (Bloomberg.com, June 26, 2014), available at http://www.bloomberg.com/news/2014-06-26/hospitals-soon-see-donuts-to-cigarette-charges-for-health.html. Similarly, the New York Times reported on "health plan prediction models" that use consumer data obtained from data brokers, such as income, marital status, and number of cars owned, to predict emergency room use and urgent care needs. See Singer, "When a Health Plan Knows How You Shop," (New York Times June 28, 2014), available at http://www.nytimes.com/2014/06/29/technology/when-a-health-plan-knows-how-you-shop.html?_r=0. This kind of information usage by HIPAA covered entities—relying on data

that is not traditionally viewed as health care information and which is widely available outside of health care contexts and for a wide variety of non-health care usages—threatens to blow up the concept of what "health information" means.

This convergence of data creation and usage is leading to an increasing debate about what should be done—if anything—about this "non-HIPAA" health care data and the application of HIPAA Privacy Rules to data that does not directly involve the provision of health care. It is clear that this debate will be ongoing and extensive. It is not clear at all what the results of the debate will be.

Therefore, companies in virtually all industries—those in the health care industry, those that create, gather, and use any kind of health care data and those companies that create and disclose data that might be used for some kind of health care purpose—all need to evaluate how this debate affects them and what their role will be in the debate (and how their behavior might need to change in the future).

Each company should think about the following questions.

First, *how might this debate proceed?*

At a minimum, there are several options. Moving from "most limited" to "broadest" in application, we could see specific proposals approaching this issue in the following ways:

- A specific set of principles applicable only to "non-HIPAA health care data" (with an obvious ambiguity about what "health care data" would mean);
- A set of principles (through an amendment to the scope of HIPAA or otherwise) that would apply to all health care data; or
- A broader general privacy law that would apply to all personal data (with or without a carve-out for data currently covered by the HIPAA rules).

The first option would address this specific problem of the generally unregulated nature of non-HIPAA health care data. The second approach would create a uniform set of standards for all health care data. The last—and clearly broadest—option would recognize the difficulty in drawing the line on what is "health care data" and would create a broad set of principles for all personal data.

With these three general approaches in mind (and recognizing that each of these can have material variations), *each company should think about how this debate (and any resulting rules) would apply to you.* Are you currently covered by the HIPAA rules, as a covered entity or business associate? Do you obtain or create health care information that is either in or out of the HIPAA structure? Do you participate in business activities involving health care data that are outside the scope of HIPAA? Would a "HIPAA-like" regulation for these "non-HIPAA" activities help or hurt your business? Are you at a competitive advantage or disadvantage because of this existing set of rules?

Last, with these impacts in mind, what should your company's role be in this debate? Would a new set of rules about this "non-HIPAA" data help or hurt your business? What do you want the outcome of this debate to be?

If there are rules for this non-HIPAA data, would you like them to be the same or different from the HIPAA principles? Would you like these rules applied more broadly to all personal data? Or is there a reasonable basis for a preference to regulate only health care data?

Conclusions

While the ultimate outcome of this debate is unclear (and may remain unclear and under debate for an extended period of time), it is clear that concerns about "non-HIPAA" health care data are not going away. There simply is too much interest in "doing something" about these issues for the discussion to stop. The debate will move forward, affected groups will make proposals, regulators will opine, and legislative hearings will be held. Industry groups may choose to develop guidelines or industry standards to forestall federal legislation. At a minimum, the policy-making "noise" on this issue should be substantial and ongoing for at least the next several years. It is clear that we are a long way from any agreement or consensus on defining any new rules to address these concerns, despite the growing consensus that there is a need to do something on these issues.

The challenge for your company is to understand these issues and how they could affect you, and to think carefully and strategically about your role in the debate and how these issues will affect your business going forward.

* * *

NOTES

37

Wiley Rein Newsletter: Big Data, Privacy, Research, and De-Identification (December 2015)

Kirk J. Nahra

WilmerHale LLP (formerly with Wiley Rein LLP)

Wiley Rein LLP

Big Data, Privacy, Research, and De-Identification

December 2015

Authors

Kirk Nahra
Partner
knahra@wileyrein.com

We are living in a new and challenging era of "big data," where an increasing volume of information is being gathered about a growing range of activities and in numerous settings where data has never been captured before. Much of this data can be "personal," or at least can be linked to other data about a person, and that's what creates the privacy challenge and information opportunity.

We will see in 2016 a continuing and evolving debate about the principles related to this Big Data. We likely will see a revised European Data Protection Directive, which will address "anonymous" data and develop legal requirements for data that is not obviously about a person, but which the European Union regulators believe may be linked to individuals in potentially troubling ways (from their perspective).

In the United States, where there is no "general" data privacy law, the challenge for companies (and regulators and policymakers) is how to build best practices for the use and disclosure of "big data" information, while maintaining consistency with applicable laws, an appropriate public position concerning data practices, and an eye toward the increasing likelihood of some new kind of law or regulation addressing some or all of the big data issues. There is a real need for companies to think about their strategy and business opportunities in this area, with a corresponding need to understand both the current regulatory environment and the likely changes in the near future.

At the same time, while these issues present ongoing and creative challenges, we also are seeing specific developments in specific areas that may impact this issue on a broader scale going forward. Two areas that will move forward in 2016 are of particular interest—the 21st Century Cures legislation that has passed the U.S. House of Representatives and is slowly moving forward in the Senate, and the proposed (and substantial) revisions to the Common Rule governing much of the "research" that is conducted in the United States. Both of these proposals present substantial challenges and can encourage or impede innovation and opportunity depending on how they are resolved. The core challenge—for these specific issues and for the big data debate

generally—is to develop appropriate privacy protections while still permitting and encouraging appropriate and beneficial opportunities from this data.

21st Century Cures

The 21st Century Cures legislation is designed to improve "innovation" in the health care industry in the United States. The massive bill covers a broad range of changes to the drug development regulatory structure and the oversight activities of the Food and Drug Administration, along with a variety of important modifications to the health care regulatory structure designed in general to stimulate health care innovation. A small piece of the legislation addresses privacy issues under the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations. These privacy revisions likely are not necessary for many of the bill's larger provisions to succeed, and, as currently written, create potentially significant privacy issues without providing substantial additional benefits.

While some of the bill's HIPAA-related provisions are useful without creating significant privacy concerns (expanding certain authorization provisions and permitting off-site access to data to develop research proposals in certain situations), there are two provisions that have not received significant attention and that can lead to material privacy risks.

First, the legislation looks at revising how data can be disclosed in general for research purposes under the "health care operations" provisions of the HIPAA Privacy Rule. The current HIPAA rules appear to distinguish between permitted data analysis for internal purposes, and disclosure of research results from this data analysis. By restricting use and disclosure of protected health information (PHI) when a covered entity is "[c]onducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines" if the "primary purpose" of the activity is "generalizable knowledge," the current rules—without any real explanation—seem to impede communication of research results. In practice, covered entities have been conservative in their view of this language, even though the rule may give more flexibility than current activities seem to indicate (for example, if internal data analysis leads to results that may be worth publishing, this publication likely was not the "primary purpose" of the initial data analysis).

While removal of this "generalizable knowledge" limitation makes sense, the proposal goes too far. The legislative "solution" to this problem to date has been to revise or clarify the Rule to allow the use and disclosure of PHI by a covered entity for research purposes, including studies whose purpose is to obtain generalizable knowledge, to be treated as the use and disclosure of such information for "health care operations." This would turn all "research," which today is governed by particular privacy rules for research studies, into "health care operations" where use and disclosure is largely unrestricted. This "opens up" data for a broad variety of research projects without the current controls that are in place for these projects. This may "solve" some of the "problem" (although it may not get more data to true "researchers"), but also opens up a wide variety of additional concerns. Privacy advocates and responsible data users need to be paying more attention to this issue.

Second, the House bill also raises issues related to how certain kinds of entities involved in research essentially can pay for access to health care data. While the legislative language is very hard to follow, the language appears to permit disclosure of any PHI to pharmaceutical companies, for their research, without any particular controls, and would at the same time permit these companies to pay unlimited amounts for these data. If this is the intent of this legislation, it goes way too far (by permitting unrestrained disclosures to pharmaceutical

companies without any new controls), and raises enormous red flags by permitting unlimited payments for these data (at least under the HIPAA rules—other health care laws also may come into play). If the proposal were streamlined in important ways—such as by limiting the scope only to limited data sets, with accompanying data use agreements—the proposal might be worth additional consideration. Today, however, the language creates privacy risks, and there has been little attention paid to these provisions in the course of the debate about the broader range of topics being addressed.

The Common Rule Proposals

The proposed revisions to the "Common Rule" governing human subjects research also focus on this innovation idea, with the goal of streamlining the regulatory process related to human subjects research, to simplify the process without increasing reasonable harms for patients and other individuals. The proposed rule, developed by the U.S. Department of Health and Human Services and 15 other federal departments and agencies, has been several years in the making, and likely will be reviewed throughout 2016 (with formal comments due in early January 2016).

Unlike the 21st Century Cures legislation, where the privacy issues take a back seat in the public debate to other topics, privacy is front and center in the Common Rule proposal. The proposal is focused on research requirements and reducing administrative burdens where these steps can be streamlined without adversely impacting individual privacy. In general, it is important to simplify the overall provisions of the Common Rule so that research can proceed more efficiently with appropriate restrictions and protections for individuals in those circumstances where those protections make sense. While there likely will be ongoing tweaks, the proposal has in general developed an appropriate balance between the clear goals of these regulations.

For example, the draft creates categories of research where it is either clear that the Common Rule provisions do not apply, or where a more streamlined approach can be implemented consistent with the goal of protecting individuals. The goal is to make clear to research entities where they do not need to follow these rules, or where the rules do not impose significant additional requirements. The agencies have done a reasonable and appropriate job of developing these categories that will provide useful guidance to research entities going forward.

In general, this proposal represents a significant step forward, and one that will permit significant new research opportunities—and streamline administrative requirements in other situations, with an appropriate balance of research benefits and patient privacy. Companies participating in research projects will want to pay close attention to this proposal as it moves forward, as it will create risks and opportunities for a wide range of companies, in the health care industry and otherwise.

The De-Identification Debate

The third component of the ongoing debate in this area involves opportunities to "de-identify" data, so that the information is no longer reasonably linked to an individual. De-identification is a concept that generates significant discussion, both in its technical aspects and as a policy issue. Some countries—Australia for example—seem to be taking the position that essentially, data can never be de-identified, and that regardless of the removal of personal identifiers, data that was originally "personal" should remain that way for purposes of regulation. The current EU proposals don't go that far, although they lean toward this approach where there are ongoing linkages among data sets tied to a person, even if the person is not reasonably identifiable.

In many other countries and settings, however, there is a broader perspective about de-identification, one that more appropriately balances the benefits of
de-identification in connection with research and public health, along with various other commercial benefits, without any meaningful impact on individual privacy. This is the general approach in the Common Rule proposals—where there are no meaningful privacy risks, the need for broader regulatory review does not exist.

The most detailed de-identification framework is spelled out in the HIPAA Privacy Rule, governing the regulation of protected health information in the United States. Under this Rule, if personal information is "de-identified" according to the regulatory process, the data is no longer identifiable and can be used and disclosed for any purpose. In order to de-identify, companies have the option of two approaches: a "safe harbor" model (not to be confused with the entirely distinct—and currently defunct—EU data transfer Safe Harbor) that requires the removal of specific identifiers, and an "expert determination" method where an expert of appropriate background and experience can review a data set and determine that there is a "low risk" of re-identification of any individual. The difficulty of this technological analysis has led to various entrepreneurial efforts to engage in sophisticated and competent de-identification, through companies like Privacy Analytics in Ottawa, Canada. We also have seen efforts by other innovative companies to address de-identification as both a "privacy protection" device and an effective information security control to protect information even when it is being held for appropriate purposes (see, for example, Anonos Inc., which has developed a patented "Dynamic De-Identification" technology to protect data and preclude privacy harms). Other companies (such as IMS Health) are thought leaders on appropriate and effective use of de-identification technologies and the public and private benefits of meaningful de-identification processes and additional safeguards.

Companies involved in the "Big Data" process will want to pay close attention to both the regulatory developments and the related technological innovations, as appropriate de-identification remains an important element in the overall goal of benefiting from data without creating undue privacy risks. Because of the volume of data generated by many companies, and the public and private opportunities that can arise from appropriate use of this data, smart de-identification has become a critical component of most companies' overall data strategy.

The Result

The ongoing discussion of big data is quite complicated, and likely will not be "resolved" anytime soon. A couple of key points are clear. The opportunities to gather data from unusual sources is clearly growing, and will continue to expand for the foreseeable future. This data will generate important and useful information to guide and improve an enormous number of activities, for both public and private benefits. And, most of this information will be useful and relevant without any need for the analysts to engage in any activity that identifies specific individuals or that creates meaningful privacy risks. So, at a minimum, data analysis using big data should be encouraged and supported, as long as there are reasonable privacy protections. These protections should include appropriate security protections (because de-identified data or other masked data is most "at risk" when there are security breaches that make this data publicly available). Opportunities to use and analyze data that has been de-identified should be encouraged, as long as reasonable de-identification practices are followed (it is clear that virtually every study that has re-identified any kind of data has been based on flawed or cursory de-identification efforts). The HIPAA standard—viewed as the gold standard of de-identification—should be encouraged as a model going forward, with the idea of appropriate controls and privacy protection steps, along with contractual and security controls, creating an environment where there is a

"small risk" of re-identifying any individuals. Policymakers should examine a potential bar on re-identification (perhaps with isolated exceptions where an individual clearly would benefit from the re-identification—e.g., the data indicates a significant but undisclosed health problem in an individual). Otherwise, de-identification should be viewed as an appropriate step to get a "win-win" from big data—beneficial opportunities to improve activities, in health care and otherwise, from this broad array of personal data without meaningful privacy risk.

NOTES

38

Kirk J. Nahra and Bethany A. Corbin, Digital Health Regulatory Gaps in the United States, Compliance Elliance Journal, Vol. 4, No. 2, pp. 21–34 (2018)

Submitted by:
Kirk J. Nahra

WilmerHale LLP

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

DIGITAL HEALTH REGULATORY GAPS IN THE UNITED STATES

Kirk J. Nahra & Bethany A. Corbin

AUTHORS

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., where he specializes in privacy and information security litigation and counseling. He is chair of the firm's Privacy Practice and assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally. He provides advice on data breaches, enforcement actions, contract negotiations, business strategy, research and de-identification issues, and privacy, data security, and cybersecurity compliance. He also works with insurers and health care industry participants in developing compliance programs and defending against government investigations into their practices. Kirk, a Certified Information Privacy Professional (CIPP/US), is a longtime member of the Board of Directors of the International Association of Privacy Professionals, and serves on the Advisory Board for the Health Law Reporter, the Privacy and Security Law Report, and the Health Care Fraud Report. He has held leadership positions with various groups within the American Health Lawyers Association and the American Bar Association Health Law Section. He is rated by Chambers USA in the nation's top-tier of privacy attorneys. Kirk can be reached at: E-mail: knahra@wileyrein.com; Phone: (202) 719-7335; Twitter: @KirkJNahrawork.

Bethany A. Corbin is a complex litigation and regulatory compliance attorney with Wiley Rein LLP in Washington, D.C. She represents health care, pharmaceutical, telecommunications, and technology clients in judicial and administrative proceedings. She is a Certified Information Privacy Professional (CIPP/US) and provides strategic advice to health care organizations concerning privacy and cybersecurity. In December, Bethany will obtain her Health Care LL.M. from Loyola University of Chicago, where she has focused her studies on the intersection of health care and technology, including the Internet of Medical Things. Bethany currently serves as the Young Lawyer Representative to the Cybersecurity and Data Privacy General Committee of the Tort, Trial, and Insurance Practice Section of the American Bar Association. Bethany can be reached at: E-mail: bcorbin@wileyrein.com; Phone: (202) 719-4418; Twitter: @BethanyACorbin.

ABSTRACT

Digital health in the United States is rapidly and continuously evolving to enhance patient care and revolutionize health care delivery. This technology offers substantial promise to both patients and providers, but lacks a comprehensive regulatory structure to ensure adequate safety and privacy. While the Department of Health and Human Services, the Food and Drug Administration, and the Federal Trade Commission regulate portions of the digital health industry, their oversight is incomplete, with numerous digital health companies falling between the cracks and assuming an unregulated status. This article analyzes the state of digital health legal and regulatory oversight in the United States, discusses how state legislatures and industry organizations have worked to fill existing legal gaps, and presents strategies for encouraging compliance for unregulated entities.

TABLE OF CONTENTS

I. INTRODUCTION 24

II. WHAT IS DIGITAL HEALTH? 24

III. DIGITAL HEALTH RISKS 25

IV. DIGITAL HEALTH LEGAL & REGULATORY FRAMEWORKS 26

A. The Health Insurance Portability and Accountability Act: Scope & Applicability 27

B. HIPAA and Digital Health Technology: Assessing the Gaps 28

C. FDA, FTC, and Medical Device Regulation 29

D. State Regulatory Frameworks 31

V. THE DANGERS OF NON-REGULATION 32

VI. ENCOURAGING COMPLIANCE 32

VII. CONCLUSION 34

I. INTRODUCTION

The boundaries and applications of digital health are rapidly evolving. From wearable fitness sensors to ingestible pills to Internet-connected pacemakers and insulin pumps, digital health has the potential to transform the health care sector and revolutionize patient care. The benefits from digital health are undeniable: patients can assume greater responsibility for the management of chronic conditions while accessing medical care at their convenience and in their own homes.[1] Technology-based health care can further reduce the costs of care and help address the physician shortage across America.[2] These benefits are a significant incentive to increase the adoption of mobile and digital technology in the health care industry, and the rate of this adoption is only projected to increase.

While digital health offers substantial promise, it suffers to some extent from a lack of comprehensive regulation. This regulatory gap presents potential concerns both for patients—who may not be provided with appropriate protections—and for the industry, which will see compliance, operational and strategic challenges in designing products that meet with existing standards, potential future regulation, and consumer and regulator expectations. Privacy laws in the United States are sectoral and patchwork in nature, and those related to health care have not been significantly revised to address technological innovation. Privacy and security for digital health applications are therefore in flux, with some subsections of the industry unregulated by federal law. This article analyzes the scope and gaps of health care privacy and security laws in the United States and discusses available privacy and cybersecurity frameworks that exist for unregulated health care actors.

II. WHAT IS DIGITAL HEALTH?

The term digital health, at its most basic, refers to the intersection of health care and the Internet. Digital technologies that fall within this category are broad, and may include mobile health (mHealth), health information technology (HIT), wearable devices, telemedicine, the Internet of Things (IoT), and personalized medicine.[3] While these technologies serve different functions—for example, HIT includes electronic health records and e-prescribing whereas IoT concerns sensors that interact between humans and machines to collect relevant health care data for diagnosis and disease management—they share one

---

1 See U.S. DEP'T HEALTH & HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 2 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf (last visited Aug. 20, 2018, 01:30 PM). [hereinafter HHS HIPAA OVERSIGHT REPORT]

2 Jeff Lagasse, *With Physician Shortage Looming, Hospitals Turn to Telehealth Tools*, HEALTHCARE FINANCE (June 1, 2018), https://www.healthcarefinancenews.com/news/physician-shortage-looming-hospitals-turn-telehealth-tools (last visited Aug. 20, 2018, 01:35 PM).

3 Charlotte A. Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 (1), ANNALS HEALTH LAW 1, 4 (2017).

fundamental overriding goal: to use technology as a method for improving health care and increase the access and quality of medical services.

The advent and adoption of digital health has the potential to profoundly impact the health care economy over the next several decades. To date, the United States has spent approximately 18% of its Gross Domestic Product on health care every year, and this figure is expected to increase to 20% by 2025.[4] Digital health, however, is simultaneously expected to grow by a compounded annual growth rate of 26% in the upcoming years, and is projected to top $379 billion by 2024.[5] These anticipated technological developments in the health care space may increase pressure to create and implement lower-cost health care solutions and incentivize companies to continue developing digital health products.[6] Significant shifts in the delivery of health care could be witnessed over the next several years.

III. DIGITAL HEALTH RISKS

Although the benefits of digital health are undeniable, concerns exist regarding the privacy and security of data collected through digital technologies. Like all digital platforms, Internet-connected health care devices pose privacy and security risks for their users. First, digital health applications collect and store patient health data, which may contain extremely sensitive information. Without proper security safeguards, this personal data may be unlawfully accessed by unauthorized users, resulting in a breach of personal information. Such a breach not only harms the business and reputation of the digital device manufacturer, but also exposes critically sensitive patient data. There is no shortage of bad actors attempting to access medical data. Indeed, health data is one of the most lucrative objects for sale on the black market, fetching higher prices than social security numbers and financial information.[7] Thus, the traditional data breach risk that is present with any Internet technology is amplified in the health care context due to value-laden sensitive data.

Second, device interoperability and network connectivity bring the possibility for new attack vectors and vulnerabilities.[8] A network hosting interconnected devices exponentially expands its attack surface such that a security flaw or breach in any device operates as a backdoor entry point into the entire system.[9] These digital health devices weaken the

4 Id. at 3.

5 Keith Speights, *What Is Digital Health?*, MOTLEY FOOL (May 9, 2017, 7:04 AM), https://www.fool.com/investing/2017/05/09/what-is-digital-health.aspx (last visited Aug. 20, 2018, 01:37 PM).

6 Tschider, supra note 3, at 4.

7 See generally PRESIDENT'S NAT'L SEC. TELECOMMUNICATIONS ADVISORY COMMITTEE, NSTAC REPORT TO THE PRESIDENT ON THE INTERNET OF THINGS ES-1 (Nov. 19, 2014), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf (last visited Oct. 23, 2018, 01:35 PM).

8 Id. at 7.

9 See id. at 1.

overall security of a medical IT network by their mere presence on the network, and further create access points that must be monitored and evaluated by the organization's technology team. Unauthorized access into a network further has the potential to compromise data integrity, which can negatively impact patient care and treatment plans.

Finally, digital health offers a unique risk that is not present with all Internet-based platforms: bodily harm. Digital health devices that are implanted into a patient's body, such as a cardiac pacemaker, may use the Internet to receive signals or instructions from a health care provider. Hijacking a pacemaker could allow an unauthorized third party to manipulate the device's functionality and cause significant bodily harm or death. This same scenario is present with digital insulin pumps, where device hijacking could alter the dose of insulin a patient receives.

Thus, digital health presents privacy, security, and resiliency risks that must be addressed and mitigated. These risks are increasingly being discussed in public policy circles, with the widespread recognition that technology advances faster than policy. The result is a crucial gap between legal frameworks and technological reality that heightens the security and privacy risks associated with digital health technology.

IV. DIGITAL HEALTH LEGAL & REGULATORY FRAMEWORKS

Digital health in the United States does not exist in an unregulated environment. Rather, the United States has adopted a sectoral approach to privacy that vests regulatory authority for the health care sector with three federal government agencies (in addition to potential regulation in each of the states): The Department of Health and Human Services (HHS), the Food and Drug Administration (FDA), and the Federal Trade Commission (FTC). In terms of privacy and security, HHS's Office for Civil Rights (OCR) plays a dominant role in its enforcement of the Health Insurance Portability and Accountability Act (HIPAA).[10] HIPAA represents the main legal framework addressing privacy and security requirements for the health care industry, and its applicability to digital health technologies is the focus of this article. In addition to HHS, the FDA regulates the efficacy and safety of medical "devices",[11] and has proposed voluntary cybersecurity guidance for connected medical devices.[12] Finally, the FTC has broad non-industry-specific enforcement powers that stem from Section 5(a) of the Federal Trade Commission Act (FTC Act).[13] Pursuant to the FTC Act, the FTC may regulate unfair and deceptive trade practices in or affecting commerce. While the FTC Act does not specifically mention privacy,

---

10 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 3.

11 Medical Device Overview, U.S. FOOD AND DRUG ADMINISTRATION (last updated Sept. 14, 2018), https://www.fda.gov/forindustry/importprogram/importbasics/regulatedproducts/ucm510630.htm (last visited Aug. 28, 2018, 01:58 PM).

12 See Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, U.S. FOOD & DRUG ADMINISTRATION (Jan. 22, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf (last visited Aug. 28, 2018, 01:53 PM).

13 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 3.

the FTC has brought numerous cases under Section 5(a) alleging that companies have engaged in deceptive acts by failing to adhere to their stated privacy policies and procedures. This article next considers the scope and gaps of these regulatory frameworks as applied to digital health technology, and discusses efforts by state legislatures to bridge these gaps.

A. The Health Insurance Portability and Accountability Act: Scope & Applicability

In 1996, Congress passed the Health Insurance Portability and Accountability Act to enhance the portability of health insurance coverage and reduce the administrative costs and burdens associated with health care delivery.[14] Neither of these primary goals were directed at privacy and security—instead, the privacy and security rules that resulted from the HIPAA law were not discussed in any substantive way in the HIPAA statute. Instead, when Congress failed to step in and create a privacy and security law, HHS (later supplemented by the Health Information Technology for Economic and Clinical Health Act (HITECH Act)), created federal regulatory protections for the privacy and security of certain health information in certain settings when held by certain entities—with the scope of these rules defined by the "non-privacy" goals of the HIPAA statute.[15] The HIPAA Privacy Rule sets forth required limitations on the use and disclosure of protected health information (PHI),[16] while the HIPAA Security Rule mandates administrative, technical, and physical safeguards for electronic PHI.[17] Essentially, HIPAA seeks to protect health information by prohibiting disclosures of information that are unlawful or unauthorized, and ensuring that applicable health care entities enact reasonable and appropriate security safeguards for the data they collect or store.

While the scope of HIPAA appears broad, its privacy and security requirements apply only to health care organizations that qualify as "covered entities."[18] A covered entity is any health plan, health care provider, or health care clearinghouse, as those terms are statutorily defined (again, driven by concerns about portability and administrative simplification and not privacy or security).[19] In 2009, the HITECH Act extended HIPAA's provisions to "business associates," which include persons or organizations that perform certain functions on behalf of a covered entity involving the use or disclosure of PHI—essentially, service providers to these covered entities where the services involve individual information.[20] PHI, in turn, is defined as individually identifiable health information

---

14 Kirk J. Nahra, *HIPAA Privacy and Security for Beginners*, WILEY REIN (July 2014), https://www.wileyrein.com/newsroom-newsletters-item-5029.html (last visited Aug. 28, 2018, 01:55 PM).

15 See id.

16 See 45 C.F.R. § 164.502; DEP'T HEALTH & HUMAN SERVS. OFFICE FOR CIVIL RIGHTS, SUMMARY OF THE HIPAA PRIVACY RULE 1 (last revised May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf?language=en (last visited Aug. 28, 2018, 02:05 PM).

17 See 45 C.F.R. §§ 164.308-312.

18 See, e.g., 45 C.F.R. § 164.502.

19 Id. § 160.103; Nahra, supra note 14.

20 See 45 C.F.R. § 160.103.

that a covered entity or its business associate holds or transmits in any form or media.[21] The foundational principle of HIPAA is that a covered entity or business associate may not use or disclose PHI except as either expressly permitted in the Privacy Rule, or as authorized by the patient in writing. A covered entity is only required to disclose PHI in two circumstances: (1) to the patient herself when requested; and (2) to HHS as part of a compliance investigation or enforcement action.[22] A covered entity is permitted—but not required—to disclose PHI without first obtaining the patient's authorization (with presumed consent under the HIPAA Privacy Rule) for the "core" purposes of the health care system—treatment, payment, and performance of health care operations (TPO) (essentially the administrative operations of a health care business).[23] There also are various "public policy" rationales for the use and disclosure of PHI. All other uses and disclosure of PHI not expressly permitted by the Privacy Rule require an individual's written authorization.

B. HIPAA and Digital Health Technology: Assessing the Gaps

Although HIPAA may appear at first blush to be a comprehensive privacy framework for the health care industry, it has significant gaps and limitations when applied to digital health technology.[24] First, HIPAA's protections only extend to digital health actors that qualify as covered entities. When HIPAA was originally drafted, HHS only had authority to create a privacy rule applicable to covered entities such as health care providers and health insurers.[25] This means organizations that do not qualify as covered entities or business associates typically have no obligation to comply with HIPAA's requirements. For example, a company manufacturing a fitness tracker that collects basic health information such as height, weight, and biometric data, would not be subject to HIPAA's regulations because the company provides this product directly to an individual consumer without the involvement of a doctor or health insurer. The company does not provide or pay the cost of an individual's medical care, does not provide medical services, and does not process non-standard data received from another entity into a standardized format (e.g., billing companies, community health management information systems, etc.). In other words, the company is not a covered entity (i.e., it is not a health plan, a health care provider, or a health care clearinghouse). Thus, this company would fall outside the bounds of HIPAA's privacy and security regulations despite the fact that it collects sensitive health data.

---

21 Id.

22 Id. § 164.502; Nahra, supra note 14.

23 45 C.F.R. § 164.502; Nahra, supra note 14.

24 See HHS HIPAA OVERSIGHT REPORT, supra note 1, at 20; Kirk J. Nahra, *What Closing the HIPAA Gaps Means for the Future of Healthcare Privacy*, HITECH ANSWERS (Nov. 9, 2015), https://www.hitechanswers.net/what-closing-the-hipaa-gaps-means-for-the-future-of-healthcare-privacy-2/ (last visited Aug. 28, 2018, 03:14 PM).

25 Nahra, supra note 24.

Second, HIPAA only protects and regulates PHI. PHI refers to individually identifiable health information (including demographic data) that relates to a person's physical or mental health, the provision of health care services to that individual, or payment for health care services, and that identifies the individual or would provide a reasonable basis for identification.[26] Health care data that does not satisfy this definition may be collected, used, and disclosed by a company without running afoul of HIPAA. For example, where health information has been de-identified or aggregated without disclosing individual identifiers, it does not constitute PHI and may be disclosed without an individual's consent or authorization.[27] In State ex rel. Cincinnati Enquirer v. Daniels, for instance, the Ohio Supreme Court held that the Cincinnati Enquirer could obtain copies of lead-contamination notices issued by the Cincinnati Health Department.[28] The court found that the notices did not reveal PHI even though they referenced an unnamed child whose blood test showed an elevated lead level.[29] Similarly, guidance on HHS's website notes that merely reporting the average age of health plan members is not PHI because the aggregated data does not identify any individual plan member.[30]

These limitations in HIPAA's scope present large regulatory gaps when applied to the digital health sector (except in those situations where a digital health product is provided directly by a HIPAA covered entity or in a business partnership with a provider or insurer). Today, with minor exceptions, most digital health companies do not qualify as covered entities or business associates, and remain unregulated by HIPAA. Similarly, some of these organizations may collect sensitive health data that does not qualify as PHI. When either of these scenarios occurs, the digital health company is not subject to HIPAA's privacy and security regulations, and may operate with significantly less federal oversight. The regulatory scheme created by HIPAA focuses largely on which entity holds the data, and not on the nature or sensitivity of the information being collected. This, in turn, allows a significant portion of the digital health sector to avoid compliance with these crucial HIPAA privacy and security standards.

C. FDA, FTC, and Medical Device Regulation

In addition to HHS's oversight of HIPAA, the Food and Drug Administration assumes a key role in the regulation of medical devices, including Internet-connected medical technology. The FDA's role, however, is limited primarily to ensuring the safety and efficacy of certain classifications of devices, and not all mobile or digital technologies will trigger

---

26 Id. § 160.103.

27 Id. § 164.502(d).

28 844 N.E.2d 1181 (Ohio 2006).

29 Id. at 523; Cuyahoga Cty. Bd. of Health v. Lipson O'Shea Legal Group, 50 N.E.3d 499, 501 (Ohio 2016)

30 Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last updated Nov. 6, 2015).

FDA scrutiny.[31] Moreover, FDA regulations are not typically geared towards protecting patient privacy or security. While the FDA has released voluntary guidance "for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices," this guidance is not mandatory.[32] The FDA does not require cybersecurity testing for any device, and relies on the device manufacturer to perform any voluntary security testing.[33] Further, the FDA does not regulate device privacy, leaving such devices to be covered (if at all) by HIPAA.

Similarly, the Federal Trade Commission has played a crucial part in privacy policy, enforcement, and best practices since the 1970s.[34] The FTC is an independent federal agency responsible for protecting consumers and promoting competition. While the FTC is not specific to health care, its regulatory authority extends to unfair and deceptive acts or practices, which may occur in the health care industry.[35] In particular, the FTC can bring enforcement actions to halt violations of privacy and security laws. The FTC has brought more than 500 enforcement actions to protect consumer privacy, and these actions address a wide range of issues, including spyware, mobile devices, file sharing, and spam.[36] Cases may also involve non-adherence to a privacy policy. Similarly, the FTC has initiated over 60 cases since 2002 against companies that failed to adequately protect consumers' personal data.[37] In this manner, FTC's authority is broad, but is not directed at preventing or regulating privacy and security standards in the health care industry. Instead, FTC acts as a watchdog to enforce existing privacy and security standards, but does not create those standards. Thus, while FTC may enforce existing privacy and security laws in the digital health context, it does not address legislative gaps that may leave digital health technology unregulated.

---

31 See Kirk J. Nahra, *New York Attorney General Addresses Key Health Care Privacy Gaps*, WILEY REIN (Apr. 2017), https://www.wileyrein.com/newsroom-newsletters-item-April_2017_PIF-NY_AG_Addresses_Key_Health_Care_Privacy_Gaps.html (last visited Aug. 28, 2018, 03:15 PM).

32 Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, U.S. FOOD & DRUG ADMINISTRATION 4 (Dec. 28, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf (last visited Aug. 28, 2018, 01:43 PM).

33 Adam Brand, *Closing the Gap in Medical Device Cybersecurity*, PROTIVITI (Jan. 3, 2018), https://blog.protiviti.com/2018/01/03/closing-gap-medical-device-cybersecurity/ (last visited Aug. 28, 2018, 01:43 PM).

34 Protecting Consumer Privacy and Security, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last visited Sept. 29, 2018, 04:33 PM).

35 See Privacy & Data Security Update:2017, FEDERAL TRADE COMMISSION, at 1 (Jan. 2017 – Dec. 2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (last visited Sept. 29, 2018, 04:19 PM).

36 Id. at 1-2.

37 Id. at 4.

D. State Regulatory Frameworks

As the gaps associated with federal legislation become more apparent, states have begun stepping in to ensure comprehensive privacy and security standards apply to digital health. In March 2017, for example, New York Attorney General Eric Schneiderman announced that his office settled three cases with various mobile health applications for insufficient or inappropriate privacy practices, and misleading privacy and security claims.[38] In bringing these cases, New York acted to fill a regulatory gap in FDA oversight—these digital health devices had not triggered FDA review—and the HIPAA Privacy Rule.[39] Specifically, although digital health devices were being used in these cases, the companies did not qualify as covered entities and, therefore, no federal privacy structure governed these organizations. The New York Attorney General stepped in to ensure privacy protections would be applicable to these digital health applications despite the absence of a comprehensive federal regulatory structure.[40] Such action signifies a potential shift toward "regulation through enforcement,"[41] which states may begin to use more frequently if federal privacy and security standards are not properly updated.

In addition to New York's enforcement action, states have also begun implementing legislation to patch the holes in federal regulations. The most recent and innovative action by a state is S.B. 327, a cybersecurity bill governing Internet of Things devices in California.[42] California Governor Jerry Brown recently signed this bill into law, making it the first state in the nation to adopt IoT legislation. This new law, which becomes effective on January 1, 2020, will mandate that any manufacturer or developer of a "smart" device—including connected health devices—ensure that the product is equipped with reasonable security features to protect the device and the information it houses.[43] Advocates of the bill hope that the new law will focus nationwide attention on the issue of IoT security, which extends beyond state boundaries.

Legislation, such as S.B. 327, is intended to bridge gaps in federal regulatory frameworks. Whereas a digital health company may escape HIPAA's grasp because it does not qualify as a covered entity, the company would still be subject to minimum privacy and security standards if it conducts business in California. The goal of such legislation is to minimize opportunities for organizations to collect sensitive data without being subject to some form of regulatory structure simply because the pace of technological innovation outpaces policy discussions.

As the nation reacts to S.B. 327, it will be interesting to observe whether other states implement comparable legislation, and whether upcoming bills will spur the federal legislature to create a comprehensive regulatory framework. Addressing privacy and security for

---

38 Nahra, supra note 31.

39 Id.

40 Id.

41 Id.

42 Senate Bill No. 327 (Cal. Sept. 28, 2018), available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 (last visited Sept. 29, 2018, 03:19 PM).

43 Id.

digital health and other Internet-connected devices on a state-by-state basis risks inconsistent standards and approaches, which could make it more difficult for digital health companies to determine their obligations, duties, and responsibilities. Comprehensive federal legislation could add consistency and predictability to privacy and security standards in digital health. However, until the federal legislature takes action, such standards will have to be developed and enforced by states and industry organizations.

V. THE DANGERS OF NON-REGULATION

Inconsistent or non-regulation of health care entities presents numerous risks that are unacceptable to both organizations and patients. Importantly, the lack of a mandatory regulatory regime may lead some digital health companies to avoid basic privacy and security practices altogether and endanger patient data. In many instances, economic incentives can cause digital health companies to push their devices to market with little consideration for security measures.[44] These devices, in turn, may be particularly susceptible to hacking, which can lead to the unauthorized acquisition of patient health data. Moreover, these devices may operate on larger health care networks and create backdoor entry points to accessing data from an entire health system that is otherwise secure. Such devices not only jeopardize the confidentiality and integrity of their own users' data, but also have the potential to create widespread breaches of health data at larger institutions.

Moreover, consumers are often not equipped to understand the difference between covered entities and non-covered entities and how this distinction drives digital health compliance. Instead, consumers may assume that their sensitive health data is protected and that adequate security measures will protect them from harm despite a contrary reality. The current regulatory framework assigns consumers the hardship of understanding the applicability of complex legal regulations to protect their own privacy and security.

Consumers, however, are not the only group harmed by gaps in digital health regulation. Digital health innovators and entrepreneurs are also adversely affected. In particular, having separate rules that apply to covered and non-covered entities can create confusion among tech innovators as to whether their products would be regulated under federal frameworks. This uncertainty may result in hesitant investors, which can delay or stifle technological innovation in the health care industry.[45] Further, a breach from lax security practices may cause immense reputational damage to the digital health company.

VI. ENCOURAGING COMPLIANCE

While federal regulatory compliance may not be mandatory for a large portion of the digital health industry, digital health companies should nonetheless ensure they are adhering to adequate privacy and security standards. The reason for this is, at a minimum, three-

---

44 See Paul Merrion, DHS Warns Insecure Internet of Things Could Spur Product Liability Lawsuits, CQ ROLL CALL WASH. DATA PRIVACY BRIEFING (Nov. 16, 2016), available at 2016 WL 6774799.

45 Alexis Guadarrama, *Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry*, 55 (4) HOUSTON LAW REVIEW 999, 1017 (2018).

fold. First, consumers expect minimum privacy and security standards to be associated with their products, and can negatively impact a company's market share if that company fails to satisfy consumer expectations. Second, it is inevitable that unregulated digital health companies will eventually be subject to a privacy and security regulatory scheme. While the form of this comprehensive regulatory framework is currently unknown, the risks associated with unregulated digital health products are too great to leave this industry unattended. This has become evident with California's implementation of S.B. 327—if the federal legislature does not act, states will. Companies that delay implementing basic privacy and security standards now will be adversely impacted if a new regulatory structure takes effect. Moreover, it is likely that regulations for digital health companies will mirror privacy and security best practices in effect today. Digital health companies have the opportunity now to build strong compliance programs and privacy policies, which will result in a smooth transition under future regulations.

Finally, by participating in the privacy and security dialogue today, digital health companies can help establish the standards and requirements for future regulations that will govern their industry. Public-private stakeholder participation is actively encouraged as policymakers think through how to regulate new technologies without stifling innovation.[46] By engaging with privacy and security concerns today, digital health companies can advocate for regulations that will promote their business interests while protecting consumer data.

The question then becomes which frameworks should digital health companies adhere to when implementing privacy and security standards? The obvious choice is HIPAA, particularly for data security, even though its requirements are not yet mandatory for a significant portion of the digital health industry. As an established framework governing health care privacy and security compliance, HIPAA contains sufficient flexibility to adapt to varied circumstances and organizations, including digital health. By voluntarily complying with HIPAA (or trying to meet its standards where they make sense for the business), digital health companies can ensure they are implementing best practice standards in effect for the health care industry. Such compliance will also create consistency across the health care sector and avoid inconsistent application of privacy and security rules. Consumers will be better able to gauge their privacy and security rights and remedies with uniform implementation of HIPAA's rules. Indeed, numerous experts have counseled in favor of expanding HIPAA's reach to the digital health industry.[47] The downside to voluntary compliance with HIPAA, however, is not only the costs associated with implementing adequate standards, but also the concern that the traditional TPO model of disclosure under HIPAA may not fit well with consumer facing products.

An alternative is for digital health companies to implement industry-created cybersecurity

---

46 See Bethany Corbin & Megan Brown, *Partnerships Can Enhance Security in Connected Health and Beyond*, CIRCLEID (Dec. 14, 2017, 8:30 AM), http://www.circleid.com/posts/20171213_partnerships_can_enhance_security_in_connected_health_and_beyond/ (last visited Sept. 30, 2018, 05:19 PM).

47 See Mary Butler, *Is HIPAA Outdated? While Coverage Gaps and Growing Breaches Raise Industry Concern, Others Argue HIPAA is Still Effective*, 88 J. AHIMA 14 (2017), http://bok.ahima.org/doc?oid=302073#.W6TW0a2ZP-Y (last visited Sept. 29, 2018, 03:19 PM).

frameworks. Many HIPAA-regulated entities also follow one or more security frameworks developed by industry professionals to enhance the security and availability of patient data. Numerous frameworks exist, enabling digital health companies to adopt the framework that best meets their organizational structure and needs. The 2018 HIMSS Report surveyed health care organizations and identified the five primary security frameworks in use throughout the health care industry today:[48] (1) National Institute of Standards and Technology (NIST);[49] (2) Health Information Trust Alliance (HITRUST);[50] (3) Center for Internet Security (CIS) Critical Security Controls;[51] (4) International Organization for Standardization (ISO);[52] and (5) Control Objectives for Information and Related Technologies (COBIT).[53] Adoption of one of these voluntary cybersecurity frameworks will assist digital health companies with remaining up-to-date on cybersecurity hygiene and can offer insight into guarding against common security threats affecting the industry

VII. CONCLUSION

Digital health represents an advantageous development to enhancing patient wellness and health care delivery in the United States. With the potential to lower medical costs and serve broader patient populations, digital health is only projected to grow in the coming years. As this technological frontier develops, it is crucial that federal regulations evolve to safeguard patient privacy and security. The current regulatory framework for the health care industry contains significant gaps that exclude a majority of digital health companies from necessary federal oversight in their data collection practices. As Congress considers the most effective method to remedy these gaps, digital health companies should be proactive in their approach to privacy and security, including voluntary compliance with HIPAA and industry-created cybersecurity frameworks. Such proactive behavior not only promotes consumer confidence in the digital health company, but also enables the company to contribute to the dialogue on best practice standards for the digital health industry.

---

48 HIMSS, *2018 Himss Cybersecurity Survey,* 18 (2018), https://www.himss.org/sites/himssorg/files/ur32196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Sept. 28, 2018, 02:49 PM).

49 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Sept. 28, 2018, 03:19 AM).

50 CSF Version 9.1, HITRUST, https://hitrustalliance.net/hitrust-csf/ (last visited Sept. 21, 2018, 10:35 AM).

51 Download the CIS Controls V7 Today, CENTER FOR INTERNET SEC., https://learn.cisecurity.org/20-controls-download (last visited Sept. 21, 2018, 11:03 AM).

52 ISO 27001 - Information security management systems, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, https://www.iso.org/isoiec-27001-information-security.html (last visited Sept. 21, 2018, 10:42 AM).

53 COBIT 4.1: Framework for IT Governance and Control, ISACA, https://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx (last visited Sept. 21, 2018, 10:44 AM).

NOTES

39

Bloomberg Law, Insight: The Top Five Health Care Privacy and Security Issues to Watch in 2019, BNA, Inc. (December 21, 2018)

Kirk J. Nahra

WilmerHale LLP

INSIGHT: The Top Five Health Care Privacy and Security Issues to Watch in 2019

Published: Dec 21 2018 06:47:36

News Story

Health care privacy and security trends for 2019 involve narrow issues like potential HIPAA changes surrounding data security, says Kirk Nahra, partner at Wiley Rein LLP. But broader trends include how non-health care companies are protecting patient data, the growth of technology companies like Amazon and Google in the health space, state and federal enforcement, and watching where health care falls in national privacy legislation debate.

By Kirk J. Nahra

By Kirk J. Nahra

(Bloomberg Law) --
While much of the public debate on the health care industry focuses on payment and treatment opportunities and reforms, broad and growing issues persist about how patient data can and should be used to transform health care. Patient privacy must be at the forefront of any ongoing discusions in 2019.

In 2019, hot topics for health care privacy and security center on potential changes to HIPAA rules, the entrance of technology players in the health field, state and federal enforcement trends, and how the health care industry will fare in the national debate on privacy legislation.

1. HIPAA Updates

The core principles for privacy and data security in the health-care industry are set out in the HIPAA Privacy and Security Rules. These rules—initially established early in the 21st century—have undergone one large modification (the HITECH statute and implementing regulations) and a small handful of otherwise modest changes.

I will be watching whether a current initiative—a “Request for Information” from the HHS Office for Civil Rights—will make significant modifications to the HIPAA Rules.

The concept behind this RFI is two-fold. First, various holdover issues still remain nine years after the implementation of the HITECH statute—like the controversial HIPAA Accounting Rule. More broadly, the RFI looks at whether HIPAA creates impediments to “coordinated care” and other areas where a broader flow of patient information should be encouraged (think opioid crisis).

While only the first step in a potentially lengthy regulatory process, we may see meaningful change to some of the core provisions of the HIPAA Rules, even in a context where it isn't clear any changes are necessary.

2. The Continued Explosion of Non-HIPAA Health Data

While the HIPAA rules provide a baseline for the traditional health care industry, HIPAA has never been an overall health information privacy law. Limited by statute, the privacy rule applies only to "covered entities," mainly health-care providers and health insurers.

Over the past decade, we have seen an explosion of new kinds of health data being gathered, accessed, and analyzed by entities not subject to the HIPAA rules, primarily (but not exclusively) in the direct to consumer context. The RFI cannot address these gaps—HHS cannot extend its regulations without congressional action outside of the set of covered entities—so currently there is a significant gap in regulatory obligations for this "non-HIPAA health data."

For consumers, these gaps create privacy risks and confusion and potentially other risks of discrimination and otherwise. For the entities gathering this highly sensitive data, there is an important challenge to act thoughtfully and responsibly even in the absence of firm governing principles. I will be watching how this issue evolves in 2019, and whether companies will appropriately safeguard this important information.

3. The Tech Companies Entering Health Care

One critical element of this "non-HIPAA" data involves the accelerating role of technology companies into the health-care field. We are seeing aggressive moves into the health-care industry—on almost a daily basis—by Amazon, Apple, and others, both to disrupt perceived failures in the current industry and to make heath information more available to consumers through a variety of additional channels.

Many of these consumer-driven activities will be outside of the HIPAA rules. Some—particularly where technology companies may be moving directly into traditional health-care industry activities—may subject these companies to new regulatory obligations. So, while the health-care industry awaits the impact of these companies entering health care from a competitive direction, from a privacy perspective we will need to see how consumer interests, loosely regulated environments and health-care disruption all combine to protect (or not protect) individual privacy interests—particularly for companies whose traditional use of personal data has not been driven by health-care industry laws or ethics.

4. Enforcement (State and Federal)

Because of these developments—and the related but ongoing concerns about the security of health-care data—I will be watching how enforcement for health-care privacy and security changes in 2019.

The HHS Office for Civil Rights generally has been quiet since the new administration took office—but recently has shown more signs of life through a series of meaningful enforcement actions. Will this continue?

In addition, we are starting to see two important kinds of state enforcement from state attorneys general—both enforcement in the regulatory gaps (primarily but not exclusively in New York) and through concerted state activity to take action under the HIPAA Rules (where state AGs have formal enforcement authority in addition

to OCR). Both of these steps present meaningful risks for companies collecting health-care data—and I will be watching whether this enforcement grows in 2019, and whether the enforcement follows current precedent or moves in more aggressive directions.

5. Health Care in the National Privacy Debate

Last, the press for national privacy legislation is moving forward aggressively, driven by the GDPR in Europe, California's new privacy law, and a variety of perceived privacy abuses.

The debate about "non-HIPAA health data" preceded this latest flurry of activity, but now has been sublimated to the broader national debate. How will the health-care industry fare in this debate? The California law generally carves out HIPAA-covered entities and business associates from coverage (although not without generating meaningful confusion).

Many of the federal proposals are directed primarily at "unregulated" activities—and therefore also leave out HIPAA entities from new regulation. Will that approach continue? Does it make sense, given HIPAA's scope limits? If there is meaningful preemption, will health-care companies want to be subject to the new law, to benefit from preemption? There are lots of moving parts on this legislation, but the health-care industry needs to make sure it is participating aggressively and thoughtfully in this ongoing debate.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., and chair of the firm's Privacy Practice. He teaches privacy law at the Washington College of Law at American University. You can contact him at knahra@wileyrein.com, and follow him on Twitter @kirkjnahrawork.

NOTES

40

Hunton Andrews Kurth LLP, Centre for Information Policy Leadership, Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice—First Report: Artificial Intelligence and Data Protection in Tension (October 10, 2018)

Submitted by:
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

Dear Colleagues:

I am delighted to provide you with this first report from the Centre for Information Policy Leadership's project on **Artificial Intelligence and Data Protection**.

In this report, we attempt to describe in clear, understandable terms: (1) what AI is and how it is being used all around us today; (2) the role that personal data plays in the development, deployment and oversight of AI; and (3) the opportunities and challenges presented by AI to data protection laws and norms.

We intend for this report to provide a level-setting backdrop for the next phase of our project—namely, working with data protection officials, industry leaders and others to identify practical ways of addressing challenges and harnessing the opportunities presented by AI and data protection. Our research to date suggests that those will include identifying best practices that organisations are already employing to ensure not only legal compliance, but also legal and ethical accountability when using personal data with AI. And they will include important ways of interpreting and applying existing data protection laws to protect privacy without unnecessarily stifling adoption of and innovation in AI, as well as considerations for future data protection laws.

We are grateful to CIPL members as well as academic and government experts for their participation in this first document, and we look forward eagerly to collaborating further on the critical effort to identify solutions and practical tools in our forthcoming report.

CIPL is often described as a bridge among diverse constituencies in the pursuit of rational, accountable, effective data protection and the responsible use of data. Never has that been needed more than in the context of AI, which already delivers extraordinary benefits to individuals and society, but precisely because of its power and impact requires even more collaborative efforts to ensure that it is developed and used in ways that respect personal privacy.

At CIPL, we are committed to that task. We eagerly welcome your ideas, your insights, and your partnership in our joint journey towards achieving that goal. For more information visit https://www.informationpolicycentre.com/ or reach out to me at bbellamy@huntonAK.com.

Sincerely,

Bojana Bellamy
President

I. Executive Summary

Artificial intelligence (AI) has rapidly developed in recent years. Today, AI tools are used widely by both private and public sector organisations around the globe, and governments around the world have expressed a commitment to AI's continued development. The capabilities of AI now and in the near future create widespread and substantial benefits for individuals, institutions and society.

However, these same technological innovations raise important issues, including questions about how to deliver practical compliance with data protection laws and norms when building and implementing AI technology and on the tension between AI and existing data protection legal requirements. As a result, we have both an opportunity and an obligation to develop principles, best practices and other accountability tools to encourage responsible data management practices, respect and even bolster data protection, and remove unnecessary roadblocks for the future development of these innovative technologies. Clarifying the application of existing data protection law on AI will be essential to ensuring that limited resources are not wasted on protecting data that does not impact individuals' privacy rights or otherwise create a risk of harm. As repeated government and regulators' reports have stressed, it cannot be a choice between the already routine benefits of AI and the protection of personal data: we must find practical ways of ensuring both.

This report will introduce artificial intelligence and some of the technologies enabled by it, as well as some of the challenges and tensions between artificial intelligence and existing data protection laws and principles. The challenges to data protection presented by AI are frequently remarked on but are often addressed only at a surface level. There is an urgent need for a more nuanced, detailed understanding of the opportunities and the issues presented by AI and of practical ways of addressing these challenges, in terms of both legal compliance and ethical issues that AI raises.

We will address specific responses and solutions to the tensions between AI and data protection laws in a separate report. These will include: (1) practices that many organisations are already using, considering new tools and accountability measures; (2) opportunities for interpreting and applying existing data protection laws to AI without stifling its development; and (3) considerations for future data protection laws that account for the demands of AI and other new technologies.

II. Introduction to Artificial Intelligence

Significant advances in the analytical capacity of modern computers are increasingly challenging data protection laws and norms. Those advances are often described as "artificial intelligence", a term that describes the broad goal of empowering "computer systems to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages".[1] This one term encompasses a wide variety of

technological innovations, each of which may present distinct challenges to existing data protection requirements.

Most AI in use today involves computer systems that perform discrete tasks—for example, playing games, recognising images or verifying identity—by identifying patterns in large amounts of data. The mathematical concept of AI dates back to the 1950s but has found real-world applications in recent years due to advances in processing power and the vast amounts of digital data available for analysis. As a result, AI almost always is associated with "big data". However, recent applications of AI, such as the use of AI to defeat CAPTCHA and Google's AlphaGo Zero that taught itself to play Go at the championship level, have occurred with minimal training data, indicating that big data may not always be linked with AI.

All of the above examples are **"narrow" AI**—AI designed to perform one task or set of tasks. Narrow AI is still complicated. As the *New York Times* noted, even narrow AI tools can be "bafflingly opaque" and "evade understanding because they involve an avalanche of statistical probability".[2] This is an obvious challenge both for building confidence in new technologies and for compliance with data protection laws.

More challenging are concerns about **artificial general intelligence**. These are "notional future AI system[s] that exhibit apparently intelligent behaviour at least as advanced as a person across the full range of cognitive tasks".[3] When a system can behave in such a way that an observer could not distinguish it from that of a human—it is said to pass the so-called "Turing Test", set out by Alan Turing in 1950. Such a capability across a wide range of tasks has not yet been achieved.

The ability of a machine to mimic the human brain has led to developments in the field of "machine learning", which Stanford University professor Andrew Ng has defined as "the science of getting computers to act without being explicitly programmed".[4] Machine learning is a subset of AI that has seen many recent developments.

Collectively, these technologies increasingly describe the reality of modern computing, and nations around the globe, from the United States and Canada to EU member states, Japan, Singapore and Australia, have showcased a commitment to be at the forefront of AI with the announcement of ambitious agendas to promote the development of AI technologies. As the European Commission noted in its recent report, *Artificial Intelligence for Europe*: "Artificial intelligence (AI) is already part of our lives—it is not science fiction. From using a virtual personal assistant to organise our working day, to travelling in a self-driving vehicle, to our phones suggesting songs or restaurants that we might like, AI is a reality". The report goes on to note the important fact that "[b]eyond making our lives easier, AI is helping us to solve some of the world's biggest challenges: from treating chronic diseases or reducing fatality rates in traffic accidents to fighting climate change or anticipating cybersecurity threats".[5] The commitment to AI is further highlighted by the creation of the EU AI Alliance, a multi-stakeholder forum created to promote discussion of all aspects of AI's advancement, as well as the AI High Level Expert

Group, which is the steering group for the AI Alliance, tasked with drafting ethical guidelines on AI by the end of 2018.[6]

AI and related technologies are rapidly advancing. "Like the steam engine or electricity in the past, AI is transforming our world, our society and our industry".[7] Thus, as the term is used below, AI encompasses narrow AI, which is widely used today and has been used for many years, as well as other digital technologies that are ushering in a future of computers so integrated into daily life that we no longer think of them as computers at all.

III. Capabilities of Artificial Intelligence

While machine learning and AI are often used interchangeably, **machine learning** is more accurately understood as one method to achieve AI. Machine learning uses statistical techniques to give computers the ability to "learn"—to progressively improve the machine's performance by creating new mathematical algorithms—from large volumes of data without being explicitly programmed. Rather than simply following instructions, as traditional computers do, machine learning makes predictions and recommendations based on patterns detected in training data sets.

Machine learning is the basis of other tools, some of which are described below, and it is widely used today to perform numerous tasks, including fraud detection, email filtering, detecting cyber threats such as network intruders or malicious insiders, recommending books or movies, or providing other services based on past or anomalous behaviour. Machine learning is the technology behind Cue, Toyota's robotic basketball player that has perfect accuracy shooting a basketball and outperforms NBA greats.[8]

Deep learning is a type of machine learning, inspired by the neural networks of the human brain to process successive layers of information and arrive at a conclusion. Deep learning uses multiple layers of artificial neural networks to simulate human decision-making. This technology is at the heart of many AI applications developed today, and enables technologies such as computer vision, text classification, pattern recognition, speech understanding and predictive recommendations. Deep learning has made it possible to have voice recognition technologies throughout our daily lives—in smartphones, digital assistants, AI-powered home security systems and other smart devices. Deep learning in the entertainment industry has enabled Walt Disney to improve significantly image quality in films, as well as improve predictions and understanding of audience reaction to certain scenes.[9] Often, deep learning uses larger data sets to create larger models and optimally train those models.

Deep learning has enabled a rise in the technology known as **computer vision**, where machines skilled at image recognition, comparison and pattern identification "see" with equal or far greater acuity than human eyes, and then connect what they see based on previously examined training data. Computer vision has created advances in healthcare, national security, assistive care and other various sectors. For example, in health care, algorithms today are able to assess

the risk of heart disease in patients by analysing blood vessels in a retina scan; detect cancerous tumours by examining CT scans; diagnose pneumonia by examining chest x-rays; and identify adult-onset diabetes by looking for patterns of retina damage.[10]

Another application of computer vision is helping visually impaired individuals understand images or better perceive their environment by describing them as text, or helping hearing-impaired individuals communicate by translating spoken words to text on a screen.[11] Perhaps the most common day-to-day application of computer vision is facial recognition, which is used for accessibility, as well as to unlock smartphones, tag pictures of friends on social media and search images.[12] Computer vision has also proven its use in sports, as auto racing uses it to improve driver safety; golf uses it to improve player experiences and analysis; and the International Gymnastics Federation plans to incorporate it in the Tokyo Olympics of 2020 to assist judges.[13]

Another form of AI technology, **Natural Language Processing (NLP)**, does exactly as the name suggests—interprets and interacts with real-time dialogue. The goal of NLP, which is often combined with speech recognition technologies, is to interact with individuals through dialogue, either reacting to prompts or providing real-time translation among languages. This technology underpins many customer service transactions, as chatbots are often the first line of service. Microsoft's AI translator is capable of translating Chinese into English with "accuracy comparable to that of a bilingual person".[14] Facebook is using unsupervised AI for language translation when training data sets are scarce, such as when translating English to Urdu.[15] Such translators have numerous applications spanning across sectors, geographical boundaries and cultural barriers. Major news media have relied on NLP-based technologies to generate thousands of news, sports and financial stories over the past two years, including more than 500 reports in the *Washington Post* about the 2017 elections.[16] Additionally, the GRE exams used for admission to graduate study in many disciplines are graded today by NLP systems.[17]

NLP and computer vision are not the only subsets of AI technologies that are driving important advancements in the field, but these two often underpin other applications of AI. For example, **robotics** combines computer vision, NLP and other technologies to train robots to "interact with the world around it in generalizable and predictable ways, … facilitate manipulation of objects in interactive environments, and … interact with people".[18] Robots are beginning to assist in healthcare, at-home care for the sick or elderly and other assistive purposes. In surgeries, robotics technology helps surgeons achieve greater precision and accuracy.

While AI is often perceived as systems acting autonomously, as is the case with home robotics or self-driving vehicles, most practical applications of AI **augment human intelligence**, serving as helpful resources in various professions and automating routine tasks. AI can augment human intelligence by assisting professionals in decision-making, resource management, safety inspection and time management. For example, AI in hospitals is used to suggest diagnoses and treatments to health professionals. In resource allocation, AI is becoming essential for determining truck or airline routes and managing deployment of law enforcement resources. To

assist safety inspectors, Intel has developed a technology to help oil rig inspectors by using AI to identify and detect bolt corrosion levels and the potential need for replacement. Finally, because AI has proved both efficient and effective at issue-spotting in legal contracts, it is used to assist lawyers, shortening the length of time it takes to perform a task, freeing up time to spend on other tasks and ideally lowering legal costs.[19]

Scholars have estimated that as many as one in five workers will have an AI acting as a co-worker by 2022.[20] In *Technology Vision 2018*, Accenture identified the "Internet of Thinking", where humans and machines work hand in hand, describing it as "bringing a new level of technological sophistication to the world".[21]

IV. Public and Private Uses of Artificial Intelligence

The remarkable developments in AI applications have led to considerable use of AI in the public and private sectors. As noted by the AI report of the UK House of Lords, "AI is a tool which is already deeply embedded in our lives".[22] As a computational tool that can enhance many decision-making processes, AI enables subject-matter experts in every sector to deliver improved services and make unprecedented breakthroughs. AI technologies facilitate commercial interactions and personalised services and products, a trend that is highly demanded by consumers and clients. Personalisation occurs in the private sector through travel management, shopper recommendations and targeted advertising, as well as for societal advancements in medical diagnosis and treatment, personalised education and efficient use of resources. The benefits of AI span across a multitude of sectors, including healthcare, marketing, legal services, automotive, human resources, sustainability, agriculture, entertainment, cybersecurity, law enforcement, military and education. Rather than providing an expansive catalogue of the benefits of AI in each of these sectors, this section will provide an overview of changes in some of the major sectors influenced by emerging AI technologies.

AI in Health and Medicine. AI in healthcare is assisting with research and prevention of diseases as well as diagnosis and treatment of patients. Microsoft's Project Premonition "aims to detect pathogens before they cause outbreaks—by turning mosquitoes into devices that collect data from animals in the environment".[23] Microsoft is developing drones that autonomously find mosquito hotspots; deploying robots to collect them; and using "cloud-scale genomics and machine learning algorithms to search for pathogens".[24] Intel's Collaborative Cancer Cloud is designed to help researchers discover new biomarkers associated with cancer diagnoses and progression.[25] In addition to assisting medical research, AI is increasingly used in applications for the practice of medicine—whether that is helping doctors find the right location to operate during surgical procedures or scanning images for early disease detection.[26]

AI in Transportation. One of the most frequently discussed applications of artificial intelligence is sensor-enabled vehicles. Many modern vehicles include AI technologies that provide assistance when backing up or changing lanes. These tools are found on trains, ships and airplanes as well—almost anything that moves. Wholly autonomous vehicles have also

increasingly become a reality, with more than 10 million miles logged on public streets by driverless vehicles designed to react to changing road conditions and traffic patterns. These sensor-enabled vehicles are transforming transportation and promising dramatic changes in private vehicle ownership and use as well as public transportation.

AI in Financial Services. Within financial services, AI is used to assess the credit of clients, back-test trading models, analyse market impact of trades, interact with customers through chatbots and for regulatory reporting.[27] In addition, AI is essential for fraud detection and prevention and is being used by financial service organisations and financial technology firms, including banks, credit card companies and other payment service providers, to combat fraud and financial crimes. It is used widely today to identify patterns of normal and unusual behaviours, spot early indicators of fraud, enable faster and more accurate financial decisions and provide financial service professionals with key information meaningfully integrated from a variety of sources. For example, Mastercard acquired Brighterion in 2017 to incorporate its AI technology for fraud prevention.[28] Using this and other technologies, Mastercard has developed algorithms and models using AI to determine the likelihood of whether a transaction is legitimate or fraudulent.

AI in Marketing. AI has proven useful in more efficient and effective marketing, helping companies produce targeted ads to consumers most likely to be interested in specific products (and, conversely, not burdening consumers with ads for products for which they have no interest). For example, Nielsen's Artificial Intelligence Marketing Cloud enables clients to "respond instantly to real-time changes in consumer behavior, resulting in more relevant content and advertising, higher levels of customer engagement and improved ROI".[29] Popular technology companies such as Amazon, Netflix, Spotify and Facebook as well as traditional retailers such as Starbucks and Walmart use AI to tailor consumer advertisements and customer experiences.

AI in Agriculture. Agriculture is another area where AI is widely utilised in raising livestock and monitoring crops. Just as the agricultural sector was an early industrial user of GPS, it is an early adopter of AI, finding numerous applications for AI technology. For example, a team of researchers developed AI algorithms to assist small cattle farmers in low-income communities. "These algorithms identify patterns for each animal. This customized analysis is then visualized on a Power BI dashboard … [machine learning], based on an expert knowledge base, provides actionable recommendations, which are sent to farmers via their mobile phones".[30] Other recent AI developments in agriculture focus on monitoring, watering and maintaining crops. For example, IBM's Watson can automatically detect and water small sections of vineyards based on data retrieved via sensors, and this technology is currently being adapted to other crop systems as well.[31] Other agricultural uses of AI include predicting the effectiveness of fertilizers as well as predicting the performance of hybrid seeds based on the genomic information and identifiers of parent lines, which may also have the potential to aid biomedical research.

AI in Education and Training. Artificial intelligence in education has the ability to transform and individualize the student experience. From an early age, teaching robotics are available to help children learn interactively. Online tutoring companies are using AI to analyse, review and tailor individual learning experiences based on techniques where each student seems most responsive.[32] AI in an intelligent tutoring system is able to use machine learning to adapt and respond to students' needs in real time. This could be used to provide tutoring sessions to secondary school students, training sessions for military personnel or various on-the-job trainings. AI is also used today to help with grading exams and preventing plagiarism in student papers and published articles. AI can be used to predict needed skills and help to connect graduates' skills with available job opportunities. For example, Pymetrics, "the Netflix-like recommendation algorithm for jobs", seeks to match individual candidates to companies and jobs based on inferences drawn from data collected during neuroscience games.[33]

AI in Cybersecurity. AI is helping organisations to monitor, detect and mitigate cybersecurity threats that increasingly face governments, industry and individuals alike. This is already helping with long-standing cybersecurity issues such as spam filters, malicious file detection and malicious website scanning.[34] Alphabet recently released Chronicle, "a cybersecurity intelligence platform that throws massive amounts of storage, processing power, and advanced analytics at cybersecurity data to accelerate the search and discovery of needles in a rapidly growing haystack".[35] AI-generated dynamic threat models help predict future attacks.[36] AI facilitates more efficient threat monitoring, detection and response.

AI for Public Authorities and Public Services. The potential benefits for AI applications to deliver more efficient government services and to assist public safety and security are expansive and have been implemented at international, national and local levels. Internationally, AI has been combined with drone footage to combat wildlife poaching and illegal logging in Uganda and Malaysia, and these technologies are expected to expand to other countries after achieving promising results.[37] AI applications assist law enforcement with fraud detection, traffic control, and algorithms to predict recidivism rates and flight risks. Using predictive crime analytics, AI has helped to efficiently deploy law enforcement.[38] AI is helping to identify key people in social networks of Los Angeles, California's homeless youth population to help mitigate the spread of HIV.[39]

While AI has seen demonstrable and numerous uses to assist public authorities, it also has a substantial capacity to aid in public services such as scientific research or conservation of important monuments. For example, researchers at NASA have partnered with technologists at Intel to develop Automated Crater Detection technology to discover craters, and even water, on the moon. Technologists at Intel are also partnering with the China Foundation for Cultural Heritage Conservation to use drones to build models of deteriorated portions of the Great Wall and use AI to scan these sections to determine the exact number of bricks needed to restore and preserve the Wall.[40]

AI for Data Protection. While some scholars have argued that AI poses a threat to data protection, others have posited that AI can offer opportunities to further bolster it. For example, AI can help companies limit or monitor who is looking at an individual's data and respond in real-time to prevent inappropriate use or theft of data. Companies are developing AI-based privacy tools, such as privacy bots that remember privacy preferences and try to make them consistent across various sites, and privacy policy scanners that attempt to read and simplify privacy policies so that users can better understand them. Polisis, which stands for "privacy policy analysis", is an AI that uses machine learning to "read a privacy policy it's never seen before and extract a readable summary, displayed in a graphic flow chart, of what kind of data a service collects, where that data could be sent, and whether a user can opt out of that collection or sharing".[41]

AI can also be useful in alerting users of suspicious websites, advertisements and other malicious activity. Companies are also using AI to prevent malicious or fake content on their online platforms. For example, Facebook is using AI to monitor and respond to fake accounts and inappropriate content on their online platforms.[42] Finally, AI is enabling companies to develop technologies that are more protective of user privacy. For example, researchers are attempting to develop machine learning techniques that evaluate encrypted data, thereby enhancing user privacy.

V. The Tension with Data Protection

While AI has enormous benefits for society, it also presents a number of challenges, including potential discrimination, antitrust issues or the impact on labor markets. Each of these important issues requires thoughtful attention, but they are beyond the scope of this report because they are the subject of other bodies of law. This report focuses exclusively on the impact that data protection law may have on AI used today and under development for use in the near future. Our next report will address practical steps for industry and regulators to manage those challenges.

A. AI and the Definition of Personal Data

Data protection laws apply when personal data is involved, although the definition of personal data can vary by jurisdiction and by statute. Furthermore, the line between what is "personal" and what is not has been blurred by the correlations and inferences that can be made from aggregated data sets. Today, information that once seemed to be non-personal now has the potential to be personal data, particularly where distinct data elements are joined together. Data users and regulators alike are faced with the difficult task of determining which data should be the subject of regulation.

The EU General Data Protection Regulation (GDPR) defines personal data as:

> any information *relating to* an identified or identifiable natural person ('data subject'); an identifiable natural person is one who *can be identified, directly or indirectly*, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[43]

Other countries also broadly define personal data. For example, under South Korea's Personal Information Protection Act, personal information means "information pertaining to any living person that makes it possible to identify such individual by their name and resident registration number, image, etc.", and specifically includes "information which, if not by itself, makes it possible to identify any specific individual if combined with other information".[44]

AI, and the variety of data sets on which it often depends, only exacerbates the challenge of determining when data protection laws apply by expanding the capability for linking data or recognising patterns of data that may render non-personal data identifiable. This is not a new discovery. As *The Economist* wrote in 2015, "the ability to compare databases threatens to make a mockery of [data] protections".[45] Simply stated, the more data available, the harder it is to de-identify it effectively.

AI expands on the ability in some settings to make non-personal data identifiable in two ways. First, it broadens the types of and demand for collected data, for example, from the sensors in cell phones, cars and other devices. Second, it provides increasingly advanced computational capabilities to work with collected data. Facial features, gate, fingerprint and other forms of biometric recognition technologies provide an apt example: this expanded data set of discrete, nearly meaningless data points provides greater opportunities for the data to be combined in a way to reliably identify individuals.

Further complexity exists because personal data may be gathered even though identification of a specific individual may not be necessary for AI to take action and make a decision. For example, the sensors in vehicles might be capable of collecting enough data about pedestrians to identify them, but identification would not be necessary to avoid hitting them. The AI only needs to determine that the object is a pedestrian; any data collected is not meant to identify a specific individual. To provide a second example, to train AI to predict the probability of heart attacks occurring in women over 50, personal health data is needed, but the identification of specific individuals is not required for the AI model's analysis.

Finally, while data protection laws attempt to protect sensitive data and similar variables, technologists would argue that algorithms need to include such data in the analysis to ensure accurate and fair results. Moreover, such data may prove useful for human intervention to review and mitigate discrimination or bias. For example, when predicting the likelihood of death in pneumonia patients, researchers at Microsoft discovered that a history of asthma resulted in a lower risk of death, likely because these individuals would seek earlier treatment.

Prior to conducting the analysis, a non-modifiable risk factor such as asthma may not have been inherently obvious or relevant in determining a lower risk of death in pneumonia patients. It is improbable that a history of asthma actually lowers the risk of death, although an AI that excluded this variable would have suggested so without easily identifying the bias. Because protected variables were left in the model, it was easier for researchers to account for them.

Understanding and resolving the scope of data protection law and principles in the rapidly changing context of AI is not an easy task, but it is essential to avoid burdening AI with unnecessary regulatory requirements or with uncertainty about whether or not regulatory requirements apply. As Singapore's Personal Data Protection Commission wrote in its recent discussion paper on AI: "Governance frameworks around AI should be technology-neutral and 'light-touch'", and should provide "regulatory clarity [for] developing AI technologies and translating them into AI solutions".[46] Clarifying the application of data protection law is also critical to ensuring that scarce resources are not wasted on protecting data that does not impact individuals' privacy rights or otherwise create a risk of harm to them.

B. Data Protection Principles and Requirements

Most data protection laws reflect long-established principles. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted in 1980, articulate eight basic principles of data protection: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability.[47] Most national data protection laws around the world include requirements based on these principles.

AI is in tension with most of these data protection principles.

Collection Limitation, Purpose Specification and Use Limitation. Most data protection laws require that there be a lawful basis for both collecting and processing data. Under the GDPR, for example, the lawful bases for processing personal data are consent, contractual performance, legal obligation, vital interests, public interests or legitimate interest.[48] It is unclear what level of detail data protection authorities will require for organisations to demonstrate that they have met a lawful basis for processing. All of these depend on an organisation knowing why the data is collected and how it will be used.

Full knowledge and articulation of purposes for processing is also required by the purpose specification and use limitation principles, which respectively provide that personal data should be collected for specified purposes and then used only for those purposes or for purposes that are compatible with the original purposes.

The challenge, as well as the opportunity, is how to comply with these requirements in the context of AI when training data may potentially yield unforeseen and sometimes unpredictable results, by advanced algorithms that are not always directed by or initially understood by their programmers and may increasingly be created only by computers.

Advancements in AI challenge the collection limitation, purpose specification and use limitation principles, but may be further advanced through the reasonable application of these principles.

Moreover, the volume and variety of data typically involved in the development and deployment of AI are enormous. AI technology can use vast amounts of diverse data to improve itself and its interaction with humans. As the Norwegian Data Protection Authority explained: "Most applications of artificial intelligence require huge volumes of data in order to learn and make intelligent decisions".[49] In fact, rather than sample data, AI often works by, in the words of the United Kingdom Information Commissioner, "collecting and analysing *all* of the data that is available".[50] Providing the necessary volume and variety of data typically requires using data from different sources, where data may have been collected for a different purpose. Denying access to some or all of that data, whether for data protection or other reasons and whether by substantive limits or transactional burdens, necessarily weakens AI and may introduce some unintended bias, because, as articulated by the Norwegian Data Protection Authority, "AI learns from *all* the data it sees".[51] If AI systems are trained on a limited dataset, representative of only a small segment of the population, these systems will propagate a biased and narrow point of view.

The potential challenge created by a rigid interpretation of these principles is exacerbated by the fact that the collection limitation, purpose specification and use limitation principles undergird most other elements of modern data protection laws. These principles are the foundation of many other legal requirements, such as the need to be transparent and provide privacy notice to individuals, or the need to obtain informed consent for certain data processing. For example, the GDPR provides that consent "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her".[52] How can consent be "specific, informed and unambiguous" if an organisation may not be fully aware of how the collected data will be used, or of all subsequent purposes of processing at the time of collection? Moreover, how can it be established by a "clear affirmative act" given the volume of data and the number of transactions involved on a daily basis?

Finally, the possible transactional burden imposed by many modern data protection regulations (for example, returning to the individual to obtain new consent for an originally unanticipated use) may slow or block beneficial uses of AI. This is true of both the development and the deployment of AI. AI works at a scale and speed far greater than envisioned by the drafters of many data protection laws. Therefore, the increasing challenge is not just how to fit these modern technologies into regulatory frameworks designed for a different world, but how to do so at a speed and scale necessary to serve the public interest.

Data Minimisation. Implicit in the OECD Guidelines, and made explicit in the GDPR and other modern data protection laws, is another widely shared principle: data minimisation. "Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed".[53] Indeed, as the Norwegian Data Protection Authority noted

in its report on *Artificial Intelligence and Privacy*: "a controller cannot use more personal data than is necessary, and that the information selected must be relevant to the purpose".[54] However, with data seen as the "basic building block of the digital economy",[55] the concept of data minimisation—that companies should keep data for as little time as possible, use only the amount and type of data necessary for the model, and only for its specified use—can be seen as counterproductive to developing AI technologies. It is difficult to know in advance "what is necessary" in a world of "surprising correlations" and computer-generated discoveries. The challenges of defining a purpose for processing and only keeping data for that purpose are exacerbated because "it is not possible to predict what the algorithm will learn", and the "purpose may also be changed as the machine learns and develops".[56]

If interpreted narrowly, data minimisation, as well as limits on data retention as discussed below, can interfere with effective assessment and oversight of AI. If you restrict access to features such as race and gender, it becomes much more difficult (perhaps impossible) to determine if the AI model is biased on those dimensions. If the model is ultimately determined to be biased, it is more difficult to repair the model if the engineers do not have access to the withheld features. One might think that not allowing access to those features would prevent bias from happening in the first place, but that is not true: usually, there are other features in the data that are being used that correlate one way or another with protected variables like race or gender, and the model will learn to be biased using these correlated features. The bias will now be buried in a sea of unknown correlation, and as a result, will be difficult to detect and repair. Researchers developing facial recognition software have discovered that access to more personal data about people from a wider variety of backgrounds, races and ethnicities improves the accuracy of facial recognition, reduces systemic bias and enhances their ability to demonstrate these to regulators.[57] These are basic demands of AI services. Therefore, it will be necessary to apply this principle in more flexible and nuanced ways when considering new technologies and their applications.

Retention Limitation. To protect personal data and promote data quality, many data protection frameworks and regulations provide for storage limitation requirements. For example, the GDPR requires that personal data shall be "kept … for no longer than is necessary for the purposes for which the personal data are processed", though personal data may be stored longer if it "will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".[58] This limitation is related to the data quality principle, as the French CNIL noted, because "data that is quite simply out of date will lead to errors or malfunctions of varying gravity depending on the sector in question, from the mere dispatch of targeted advertising that does not match my actual profile, to an incorrect medical diagnosis".[59] And it implicates also rights of individuals, such as the "right to be forgotten",[60] which has found both judicial and regulatory support in Europe and elsewhere, and the right to restriction of processing.[61]

The underlying tension is that setting short retention periods and deleting or restricting the use of data after its original purpose has been fulfilled or upon request by an individual would strip organisations and society of the potential benefits of using that data for AI training, deployment and oversight. AI and machine learning technologies allow these models to perform optimally. Yet, keeping data for longer periods or indefinitely may violate current data protection laws in the eyes of regulators.

Transparency. The openness and individual participation principles require that data processing be transparent and that individuals are informed about uses of their personal data. The GDPR demands that controllers describe their data processing in greater detail and with concise, intelligible and easily accessible information. The law specifically requires processing to be transparent and further requires organisations to provide individuals the specifics of data processing, including the logic behind any automated decision-making that has legal effect or a similarly significant impact on individuals.[62] These can be difficult requirements to meet with respect to decisions made by complex AI algorithms, which are often unanticipated.

Data protection principles of transparency and openness are challenged in AI by what many refer to as the "black box" problem. This phenomenon occurs where, as described by the Norwegian Data Protection Authority, the "advanced technology employed is difficult to understand and explain", and where the neural networks—or successive layers within the technology—make it "practically impossible to explain how information is correlated and weighted in a specific process".[63] This is particularly concerning due to a fear of algorithmic bias. As the AI Forum of New Zealand explained, "AI systems are fed training data by their creators. If this data contains bias, then clearly the system will learn the same bias".[64] Inside a "black box", detecting and understanding the presence of bias is more difficult.

Providing transparency in light of the "black box" phenomenon has been one of the major topics of AI discussed by policymakers, academics and researchers. As Georgetown professor Paul Ohm has stressed, when a program "thrives on surprising correlations and produces inferences and predictions that defy human understanding … [h]ow can you provide notice about the unpredictable and unexplainable?"[65] Moreover, the opacity often found in AI models has led many countries to reaffirm a need for transparency in data protection regimes. The French Commission Nationale de l'Informatique et des Libertés (CNIL) recently articulated a "principle of continued attention and vigilance", noting that this principle could "offset the phenomenon of excessive trust and weakened accountability which can arise in front of 'black box' algorithms".[66] Technology companies are also working on ways to develop explainable AI, which would also enhance the transparency principle.

Data Quality, Access and Correction. Another consideration with AI and decision-making is data quality and the need for individuals to be able to identify and correct their data. AI technology, like any data-driven technology, can be hindered by inaccurate, incomplete or non-representative data sets, so by making decisions in a "black box", accuracy and fairness become

a substantial concern. As Singapore's Personal Data Protection Commission recently explained in a discussion paper on AI, data accountability and accuracy are impacted by "the completeness of the data required, how recently the data was collected and updated, whether the data is structured in a machine-understandable form, and the source of the data".[67] In its Technology Vision 2018, Accenture identifies the trend of "Data Veracity", explaining that "the potential harm from bad data can become an enterprise level existential threat".[68]

When decisions are made using AI, it can be challenging to contest given the complexity of an algorithm—even if some of the data points used to make the decision were incorrect. There is, however, incentive for both AI developers and privacy advocates to address this challenge. AI developers would like to have the most accurate data possible to promote trustworthiness in outcomes. Individuals would like to ensure that the algorithm will not produce a negative outcome based on incorrect, incomplete or insufficient data.

C. Automated Decision-Making and Profiling

The GDPR is distinctive among most data protection laws in that it specifically addresses profiling and automated decision-making and imposes special restrictions on certain forms of solely automated decision-making under Article 22.

Profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[69] All of the GDPR requirements apply to profiling, as they would to any other form of processing. Article 21 of the GDPR, however, specifically mentions profiling with regard to the right to object.

Similarly, all of the GDPR requirements apply to automated decision-making, though special rules exist for solely automated decision-making. Article 22 provides that an individual has the "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[70] Article 22 reflects the risk-based approach of the GDPR and subjects these significant legal or similar decisions to a higher compliance bar. This is driven by a concern for algorithmic bias; a worry of incorrect or unsubstantiated solely automated decisions based on inaccurate or incomplete data; and the need for individuals to have redress and the ability to contest a decision if an algorithm is incorrect or unfair. There is a concern that AI technology can reinforce or reflect human biases when making decisions.[71]

The Article 29 Working Party has provided Guidelines on Automated Decision-Making[72] that interpret Article 22 as a direct prohibition on such automated decision-making absent the existence of one of three exceptions provided by Article 22(2). This interpretation further limits the number of legal bases that can be used for automated decision-making and notably

prevents the use of legitimate interest as a basis for processing when making such automated decisions.

Article 22 of the GDPR also gives rights to individuals to contest the decision and seek human intervention and review.[73] Although one attribute of AI in many settings is the ability to act without human intervention, Article 22 exists to address a concern that handing over full decision-making authority to a machine where its decisional output can produce legal or similarly significant consequences for an individual is potentially harmful and dangerous. Article 22 acts to limit such consequences by providing individuals with the right not to be subject to such automated decision-making and with recourse to human intervention under Article 22(3).

However, it is crucial to understand what constitutes a "legal or similarly significant effect" to prevent stifling of AI innovation and operation. The WP29 guidelines reflect this understanding by noting that "only serious impactful effects will be covered by Article 22".[74]

Furthermore, the WP29 Guidelines highlight how difficult it may be to avoid the tension between AI and automated decision-making. For example, the Guidelines provide that "[c]ontrollers seeking to rely upon consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to, and remember that consent is not always an appropriate basis for the processing".[75] Therefore, consent may not be an acceptable basis, and in cases when it could be, organisations will have to overcome the challenges already noted with providing sufficient information about AI.

Finally, in its guidelines, the WP29 notes that "[w]hilst there can be advantages to retaining data in the case of profiling, since there will be more data for the algorithm to learn from, controllers must comply with the data minimisation principle when they collect personal data and ensure that they retain those personal data for no longer than is necessary for and proportionate to the purposes for which the personal data are processed".[76] The inherent challenge is determining when the purpose ends in relation to an AI application. Storing data indefinitely within a profile is inherent to many applications, and one can argue that it is ultimately more advantageous to individuals in the sense that the more data that is taken into account by a profiling algorithm or automated decision-making process, the more accurate the result will be.

VI. Observations

This First Report has highlighted the capabilities and benefits of AI as well as some of the tensions and challenges presented by the interaction between AI and data protection law. From this discussion, six general observations emerge.

1. **Not all AI is the same.** As we have seen, the term AI is applied to myriad technologies and applications, designed to be used in diverse settings with widely varying consequences. While a computer playing chess has a finite (although large) number of

moves to learn, a computer aiding in surgery could use an infinite amount of training data to perform optimally. Additionally, if an algorithm playing chess makes a mistake, the harm is trivial compared to the substantial harm that could result from AI producing an unexpected result during surgery. While it is possible to make high-level observations about AI generally, when it comes to applying laws and ethical principles, specificity about technologies, applications, contexts and consequences does matter.

2. **AI is widely used in society today and is of significant economic and societal value.** AI is not a new or futuristic concept; it is prevalent today and something individuals interact with constantly in mobile devices, vehicles, homes and businesses. Governments and companies around the world are rapidly investing in AI because of the reality of its substantial benefits in health, commerce, trade, public safety and other areas. This does not mean that AI does not present important issues that must be addressed, but rather that now is the time to consider practical data protection compliance. Equally, it would be counterproductive to impose unnecessary barriers to its development or to the vast amounts of data on which it depends.

3. **AI requires substantial amounts of data to perform optimally.** Data is the oxygen of AI. AI requires data to train algorithms and increase accuracy and overall functionality. With few exceptions, more data is better than less, and there is almost never enough. This is necessary not only for AI to achieve its full potential, but also, as we have seen and is described further below, to guard against bias or error and to prevent monopolization of critical AI. As Oxford University Professor Viktor Mayer-Schönberger recently noted in *Foreign Affairs*, even large companies are in need of more data to develop and deploy AI, as "the quality of [AI applications] would deteriorate absent sufficient data, leading to inefficient transactions and reduced consumer welfare".[77] This is especially true if AI is to serve the needs of small but vital subsets of the population.

4. **AI requires data to identify and guard against bias.** AI, like the humans who develop it, is not free from bias or error. However, it has the potential to avoid many of the irrational biases that infect human decision-making and to make detecting bias and errors easier and more reliable. However, as we have seen, to do this AI requires access to extensive data, especially including sensitive or protected data. Data on race, ethnicity, gender and other sensitive attributes may assist in the detection and remedy of bias or discrimination in AI (and other) models. Denying access to or preventing retention of such data will only make it harder to detect and remedy bias while also denying all segments of society the full potential of AI's benefits. At the same time, it is important to carefully control the availability and use of such data to ensure that it is not used to facilitate discrimination.

5. **The role of human oversight of AI is likely to and will need to change for AI to deliver the greatest benefit to humankind.** Society must make intelligent, well-informed and thoughtful decisions about the role of AI, but as the speed, accuracy and impact of AI

increases, the role of human oversight will need to change. Although many current applications of AI are designed to augment human intelligence, in the face of autonomous, rapid AI, human intervention may be not only unnecessary but counterproductive. Human decision-making is sometimes unexplainable or irrational. We should aspire for AI to operate more efficiently and accurately than humans, and to make less biased, more rational and reliable decisions. Individuals may not always understand how specific AI works, but they can assure that it is developed according to legal and ethical principles. Humans are essential to evaluating its results and providing redress in the case of incorrect or unfair decisions.

6. **AI challenges some requirements of data protection law.** Companies can and must strive to comply with data protection law as it currently exists. Given the distinctive characteristics of AI, this will require forward-thinking practices by companies and reasonable interpretation of existing laws by regulators if individuals are to be protected effectively and society is to enjoy the benefits of advanced AI tools. In addition, as new data protection laws are adopted, there will also be an opportunity to consider whether there are more effective approaches to protecting privacy in the context of AI and other new technologies. Many technological advances—the proliferation of mobile devices, the growth of IOT, the advent of big data—have already posed challenges to parts of the OECD Guidelines and the laws based on them. AI is likely to exacerbate those challenges, but it also creates opportunities for including more creative approaches in new laws to ensure that the public enjoys the benefits of advanced technologies while also having confidence that individual privacy is assured.

In CIPL's Second Report on Delivering Sustainable AI Accountability in Practice, we will address some of the critical tools that companies and organisations are starting to develop and implement to promote accountability for their use of AI within existing legal and ethical frameworks, as well as reasonable interpretations of existing principles and laws that regulators can employ to achieve efficient, effective privacy protection in the AI context. Finally, it will discuss considerations for the development of future data protection laws that account for the development of AI and other innovative technologies.

REFERENCES

[1] English Oxford Living Dictionaries, "Artificial Intelligence", available at https://en.oxforddictionaries.com/definition/artificial_intelligence.

[2] Kuang, C., Can A.I. Be Taught to Explain Itself?, New York Times Magazine (21 November 2017), available at https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html?_r=0.

[3] Executive Office of the President of the United States, National Science and Technology Council Committee on Technology, Preparing for the Future of Artificial Intelligence (October 2016), available at https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

[4] Machine Learning, Coursera, available at https://www.coursera.org/learn/machine-learning.

[5] Communication from the Commission, Artificial Intelligence for Europe, COM (2018) 237 final, available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625.

[6] High Level Expert Group on Artificial Intelligence, (14 June 2018), available at https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

[7] Id.

[8] Camparo, A., This basketball-playing robot is so good it could outshoot Stephen Curry, nbcnews.com (20 March 2018), available at https://www.nbcnews.com/mach/science/basketball-playing-robot-so-good-it-could-outshoot-stephen-curry-ncna858011.

[9] Rayo, E., Artificial Intelligence at Disney, Viacom, and Other Entertainment Giants, TechEmergence (11 February 2018), available at https://www.techemergence.com/ai-at-disney-viacom-and-other-entertainment-giants/.

[10] Timmer, J., AI trained to spot heart disease risks using retina scan, arstechnica.com (24 February 2018), available at https://arstechnica.com/science/2018/02/ai-trained-to-spot-heart-disease-risks-using-retina-scan/.

[11] Seeing AI App, Microsoft Accessibility Blog (12 July 2017), available at https://blogs.msdn.microsoft.com/accessibility/2017/07/12/seeing-ai-app-is-now-available-in-the-ios-app-store/; Zee, S., Whose Sign Is It Anyway? AI Translates Sign Language Into Text, blogs.nvidia.com (11 May 2017), available at https://blogs.nvidia.com/blog/2017/05/11/ai-translates-sign-language/.

[12] Quiñonero Candela, J., Managing Your Identity on Facebook With Face Recognition Technology, Facebook Newsroom (19 December 2017), available at https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/.

[13] Greenberg, N., PGA Tour Is Embracing Artificial Intelligence, And It Could Change How You Watch Golf, The Roanoke Times (8 July 2018), available at https://www.roanoke.com/washingtonpost/sports/pga-tour-is-embracing-artificial-intelligence-and-it-could-change/article_f46d97b1-0b99-5495-a9e9-a015d0b9620b.html.

[14] Del Bello, L., AI Translates News Just as Well as a Human Would, futurism.com (16 March 2018), available at https://futurism.com/ai-translator-microsoft/.

[15] Johnson, K., Facebook is using unsupervised machine learning for translations, Venture Beat (31 August 2018), available at https://venturebeat.com/2018/08/31/facebook-is-using-unsupervised-machine-learning-for-translations/.

[16] Keohane, J., What News-Writing Bots Mean for the Future of Journalism, Wired (16 January 2017), available at https://www.wired.com/2017/02/robots-wrote-this-story/.

[17] Hardesty, L., Is MIT Giving Away the Farm?, MIT Technology Review (21 August 2012), available at https://www.technologyreview.com/s/428698/is-mit-giving-away-the-farm/.

[18] Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., Hirschberg, J., Kalyanakrishnan, S., Kamar, E., Kraus, S., Leyton-Brown, K., Parkes, D., Press, W., Saxenian, A., Shah, J., Tambe, M., and Teller, A., "Artificial Intelligence and Life in 2030". One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel, Stanford University, (September 2016), available at https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf.

[19] Chin, M., An AI just beat top lawyers at their own game, Mashable (26 February 2018), available at https://mashable-com.cdn.ampproject.org/c/s/mashable.com/2018/02/26/ai-beats-humans-at-contracts.amp.

[20] Meister, J., AI Plus Human Intelligence Is The Future Of Work, Forbes.com (11 January 2018), available at https://www.forbes.com/sites/jeannemeister/2018/01/11/ai-plus-human-intelligence-is-the-future-of-work/#789369cf2bba.

[21] Accenture Technology Vision 2018 Intelligent Enterprise Unleashed (February 2018), at page 14, available at https://www.accenture.com/t20180227T215953Z__w__/us-en/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50.

[22] House of Lords Select Committee in Artificial Intelligence, AI in the UK: Ready, Willing and Able?, HL Paper 100 (2018), available at https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.

[23] Project Premonition aims to detect pathogens before they cause outbreaks, Microsoft Project Premonition (Established 2 March 2015), available at https://www.microsoft.com/en-us/research/project/project-premonition/#.

[24] Id.

[25] Artificial Intelligence, The Public Policy Opportunity, Intel (18 October 2017), available at https://blogs.intel.com/policy/files/2017/10/Intel-Artificial-Intelligence-Public-Policy-White-Paper-2017.pdf.

[26] Project InnerEye – Medical Imaging AI to Empower Clinicians, Microsoft Project InnerEye (Established 7 October 2008), available at https://www.microsoft.com/en-us/research/project/medical-image-analysis/; Novartis Cataracts Surgery; Google Retina Scan.

[27] Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services, Market Developments and Financial Stability Implications, Report (1 November 2017), available at http://www.fsb.org/wp-content/uploads/P011117.pdf.

[28] Bary, E., Visa and Mastercard Earnings: More Than Just Payments at Play, MarketWatch (25 July 2018), available at https://www.marketwatch.com/story/visa-and-mastercard-earnings-more-than-just-payments-at-play-2018-07-23.

[29] Nielsen Launches Artificial Intelligence Technology, Nielsen.com (4 April 2017), available at http://www.nielsen.com/us/en/press-room/2017/nielsen-launches-artificial-intelligence-technology.html.

[30] Spencer, G., Buffaloes and the Cloud: Students turn to tech to save poor farming families, news.microsoft.com (27 September 2017), available at https://news.microsoft.com/apac/features/saving-farming-families-tech-one-cow-goat-buffalo-time/.

[31] Vanian, J., How IBM is Bringing Watson to Wine, fortune.com (9 January 2016), available at http://fortune.com/2016/01/09/ibm-bringing-watson-wine/.

[32] Devlin, H., Could online tutors and artificial intelligence be the future of teaching?, The Guardian (26 December 2016), available at https://www.theguardian.com/technology/2016/dec/26/could-online-tutors-and-artificial-intelligence-be-the-future-of-teaching.

[33] Hiring Based in Neuroscience + Data Science, Pymetrics, available at https://www.pymetrics.com/science/.

[34] Tully, P., Using defensive AI to strip cyberattackers of their advantage, venturebeat.com (6 March 2018), available at https://venturebeat.com/2018/03/06/using-defensive-ai-to-strip-cyberattackers-of-their-advantage/.

[35] Oltsik, J., Artificial intelligence and cybersecurity: The real deal, csoonline.com (25 January 2018), available at https://www.csoonline.com/article/3250850/security/artificial-intelligence-and-cybersecurity-the-real-deal.html.

[36] Supra note 3.

[37] Kratochwill, L., Artificial Intelligence Fights Wildlife Poaching, popsci.com (22 April 2016), available at https://www.popsci.com/national-science-foundation-fights-poaching-with-artificial-intelligence.

[38] Rieland, R., Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?, Smithsonian.com (5 March 2018), available at https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/.

[39] Clay, J., USC researcher, and AI, give homeless youth a helping hand with HIV education, USC News (14 July 2017), available at https://news.usc.edu/124831/usc-researcher-and-ai-give-homeless-youth-a-helping-hand-with-hiv-education/.

[40] Intel Technology Aids in Preserving the Great Wall of China (16 July 2018), available at https://newsroom.intel.com/news/intel-technology-aids-preserving-great-wall-china/.

[41] Greenberg, A., An AI That Reads Privacy Policies So That You Don't Have To, wired.com (9 February 2018), available at https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/.

[42] For example, Facebook uses machine learning to detect and block millions of fake accounts every day by analyzing certain suspicious behaviours without ever assessing the content itself. The company also uses AI to identify and remove terrorist propaganda before it is ever reported by users. In fact, 99 percent of ISIS and Al Qaeda related terror content is removed from Facebook before the online community has flagged it. Community Standards Enforcement Preliminary Report, Facebook (2018), available at https://transparency.facebook.com/community-standards-enforcement#terrorist-propaganda.

[43] GDPR, article 4(1).

[44] Article 2(1) South Korea Personal Information Protection Act, official English translation available at http://law.go.kr/engLsSc.do?menuId=0&subMenu=5&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95#.

[45] We'll See You, Anon., The Economist (13 August 2015), available at https://www.economist.com/science-and-technology/2015/08/13/well-see-you-anon.

[46] Singapore Personal Data Protection Commission, "Discussion Paper on Artificial Intelligence (AI) and Personal Data—Fostering Responsible Development and Adoption of AI", (5 June 2018), at pages 2-3, available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Discussion-Paper-on-AI-and-PD---050618.pdf.

[47] OECD Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), available at http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[48] GDPR, article 6(1).

[49] Artificial Intelligence and Privacy, Datatilsynet (Norwegian Data Protection Authority) at page 4 (January 2018), available at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

[50] Big Data, Artificial Intelligence, Machine Learning and Data Protection, United Kingdom Information Commissioner's Office at page 11 (Version 2.2 - 2017) (emphasis added), available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

[51] Supra note 49 at page 5 (emphasis added).

[52] GDPR, recital 32.

[53] GDPR, recital 39; article 5(1)(c).

[54] Supra note 49 at page 18.

[55] Supra note 46 at page 2.

[56] Supra note 49 at page 18.

[57] Roach, J., Microsoft improves facial recognition technology to perform well across all skin tones, genders, Microsoft AI Blog (26 June 2018), available at https://blogs.microsoft.com/ai/gender-skin-tone-facial-recognition-improvement/.

[58] GDPR, article 5(1)(e).

[59] Commission Nationale de l'Informatique et des Libertés, "How Can Humans Keep the Upper Hand?: The Ethical Matters Raised by Algorithms and Artificial Intelligence", (December 2017), at page 39, available at https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf.

[60] GDPR, article 17.

[61] GDPR, article 18.

[62] GDPR, article 12 (transparency); article 13 and 14 (notice); and article 22 (right not to be subject to automated decision-making).

[63] Supra note 49 at page 19.

[64] Artificial Intelligence Forum of New Zealand, Artificial Intelligence: Shaping a Future New Zealand (March 2018), at page 64, available at http://resources.aiforum.org.nz/AI+Shaping+A+Future+New+Zealand+Report+2018.pdf.

[65] Ohm, P., "Changing the Rules: General Principles for Data Use and Analysis", Privacy, Big Data, and the Public Good: Frameworks for Engagement at page 100 (2014).

[66] Supra note 59 at page 50.

[67] Supra note 46 at page 9.

[68] Supra note 21 at page 40.

[69] GDPR, article 4(4).

[70] GDPR, article 22.

[71] Krigsman, M., Artificial Intelligence and Privacy Engineering: Why It Matters NOW, zdnet.com (18 June 2017), available at http://www.zdnet.com/article/artificial-intelligence-and-privacy-engineering-why-it-matters-now/.

[72] Article 29 Data Protection Working Party, WP251 Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (last Revised and Adopted on 6 February 2018) at page 19, available at http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826.

[73] GDPR, article 22(3).

[74] Supra note 72 at page 21.

[75] Id.

[76] Id., at page 12.

[77] Mayer-Schönberger, V., and Range, T., "A Big Choice for Big Tech: Share Data or Suffer the Consequences", *Foreign Affairs* (Sept./Oct. 2018), p. 52.

NOTES

41

Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679 (October 4, 2017)

Submitted by:
Lara Kehoe Hoffman
Netflix

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 248 rev.01

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Adopted on 4 April 2017

As last Revised and Adopted on 4 October 2017

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 03/075.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

Table of content

I. INTRODUCTION **4**

II. SCOPE OF THE GUIDELINES **4**

III. DPIA: THE REGULATION EXPLAINED **6**

A. WHAT DOES A DPIA ADDRESS? A SINGLE PROCESSING OPERATION OR A SET OF SIMILAR PROCESSING OPERATIONS. 7

B. WHICH PROCESSING OPERATIONS ARE SUBJECT TO A DPIA? APART FROM EXCEPTIONS, WHERE THEY ARE "*LIKELY TO RESULT IN A HIGH RISK*" 8

a) When is a DPIA mandatory? When processing is "likely to result in a high risk". *8*

b) When isn't a DPIA required? When the processing is not "likely to result in a high risk", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required. *12*

C. WHAT ABOUT ALREADY EXISTING PROCESSING OPERATIONS? DPIAS ARE REQUIRED IN SOME CIRCUMSTANCES. 13

D. HOW TO CARRY OUT A DPIA? 14

a) At what moment should a DPIA be carried out? Prior to the processing. *14*

b) Who is obliged to carry out the DPIA? The controller, with the DPO and processors. *14*

c) What is the methodology to carry out a DPIA? Different methodologies but common criteria. *15*

d) Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA. *18*

E. WHEN SHALL THE SUPERVISORY AUTHORITY BE CONSULTED? WHEN THE RESIDUAL RISKS ARE HIGH. 18

IV. CONCLUSIONS AND RECOMMENDATIONS **19**

ANNEX 1 – EXAMPLES OF EXISTING EU DPIA FRAMEWORKS **21**

ANNEX 2 – CRITERIA FOR AN ACCEPTABLE DPIA **22**

I. Introduction

Regulation 2016/679[1] (GDPR) will apply from 25 May 2018. Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA[2]), as does Directive 2016/680[3].

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data[4] by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24)[5]. In other words, **a DPIA is a process for building and demonstrating compliance**.

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

II. Scope of the Guidelines

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] The term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept.

[3] Article 27 of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, also states that a privacy impact assessment is needed for "*the processing is likely to result in a high risk to the rights and freedoms of natural persons*".

[4] The GDPR does not formally define the concept of a DPIA as such, but

- its minimal content is specified by Article 35(7) as follows:
  - "*(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
  - *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
  - *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
  - *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned";*
- its meaning and role is clarified by recital 84 as follows: "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk".*

[5] See also recital 84: "*The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation*".

These Guidelines take account of:

- the Article 29 Data Protection Working Party (WP29) Statement 14/EN WP 218[6];
- the WP29 Guidelines on Data Protection Officer 16/EN WP 243[7];
- the WP29 Opinion on Purpose limitation 13/EN WP 203[8];
- international standards[9].

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1)). In order to ensure a consistent interpretation of the circumstances in which a DPIA is mandatory (Article 35(3)), the present guidelines firstly aim to clarify this notion and provide criteria for the lists to be adopted by Data Protection Authorities (DPAs) under Article 35(4).

According to Article 70(1)(e), the European Data Protection Board (EDPB) will be able to issue guidelines, recommendations and best practices in order to encourage a consistent application of the GDPR. The purpose of this document is to anticipate such future work of the EDPB and therefore to clarify the relevant provisions of the GDPR in order to help controllers to comply with the law and to provide legal certainty for controllers who are required to carry out a DPIA.

These Guidelines also seek to promote the development of:

- a common European Union list of processing operations for which a DPIA is mandatory (Article 35(4));
- a common EU list of processing operations for which a DPIA is not necessary (Article 35(5));
- common criteria on the methodology for carrying out a DPIA (Article 35(5));
- common criteria for specifying when the supervisory authority shall be consulted (Article 36(1));
- recommendations, where possible, building on the experience gained in EU Member States.

[6] WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks adopted on 30 May 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] WP29 Guidelines on Data Protection Officer 16/EN WP 243 Adopted on 13 December 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] WP29 Opinion 03/2013 on purpose limitation 13/EN WP 203Adopted on 2 April 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] e.g. ISO 31000:2009, *Risk management — Principles and guidelines*, International Organization for Standardization (ISO) ; ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

III. DPIA: the Regulation explained

The GDPR requires controllers to implement appropriate measures to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the "the risks of varying likelihood and severity for the rights and freedoms of natural persons" (article 24 (1)). The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks[10] presented by the processing of personal data.

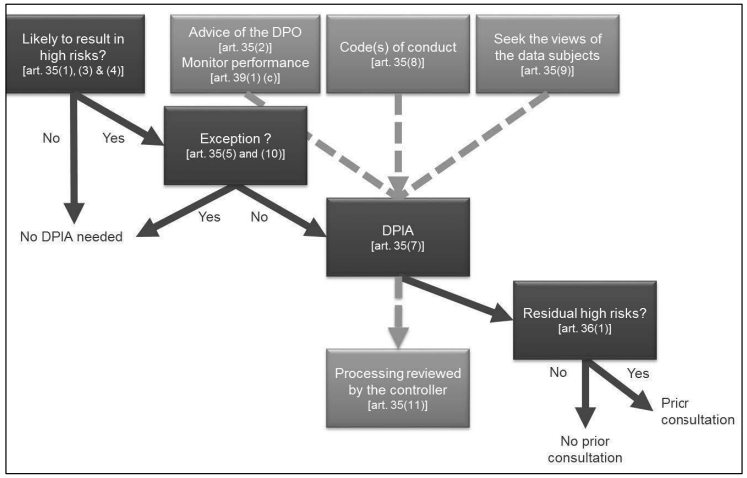
A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. "Risk management", on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.

Article 35 refers to a likely high risk "to the rights and freedoms of individuals". As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. Instead, a DPIA is only required where a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). The mere fact that the conditions triggering the obligation to carry out DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects. In practice, this means that controllers must continuously assess the risks created by their processing activities in order to identify when a type of processing is "likely to result in a high risk to the rights and freedoms of natural persons".

[10] It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to identified, analyzed, estimated, evaluated, treated (e.g. mitigated...), and reviewed regularly. Controllers cannot escape their responsibility by covering risks under insurance policies.

The following figure illustrates the basic principles related to the DPIA in the GDPR:



A. What does a DPIA address? A single processing operation or a set of similar processing operations.

A DPIA may concern a single data processing operation. However, Article 35(1) states that "*a single assessment may address a set of similar processing operations that present similar high risks*". Recital 92 adds that "*there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity*".

A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided.

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures

designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate. An example could be the relationship between manufacturers of smart meters and utility companies. Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities.

B. Which processing operations are subject to a DPIA? Apart from exceptions, where they are "*likely to result in a high risk*".

This section describes when a DPIA is mandatory, and when it is not necessary to carry out a DPIA.

Unless the processing operation meets an exception (III.B.a), a DPIA has to be carried out where a processing operation is "*likely to result in a high risk*" (III.B.b).

a) When is a DPIA mandatory? When processing is "*likely to result in a high risk*".

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1), illustrated by Article 35(3) and complemented by Article 35(4)). It is particularly relevant when a new data processing technology is being introduced[11].

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help controllers comply with data protection law.

Even though a DPIA could be required in other circumstances, Article 35(3) provides some examples when a processing operation is "*likely to result in high risks*":

- "*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person[12];*
- *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10[13]; or*
- *(c) a systematic monitoring of a publicly accessible area on a large scale*".

[11] See recitals 89, 91 and Article 35(1) and (3) for further examples.

[12] See recital 71: "*in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles*".

[13] See recital 75: "*where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures*".

As the words "*in particular*" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to DPIAs. For this reason, the criteria developed below sometimes go beyond a simple explanation of what should be understood by the three examples given in Article 35(3) GDPR.

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91, and other GDPR references to "*likely to result in a high risk*" processing operations[14], the following nine criteria should be considered.

1. Evaluation or scoring, including profiling and predicting, especially from *"aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements"* (recitals 71 and 91). Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling.
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))[15]. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).
4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms

[14] See e.g. recitals 75, 76, 92, 116.

[15] The WP29 interprets "*systematic*" as meaning one or more of the following (see the WP29 Guidelines on Data Protection Officer 16/EN WP 243):

- occurring according to a system;
- pre-arranged, organised or methodical;
- taking place as part of a general plan for data collection;
- carried out as part of a strategy.

The WP29 interprets "*publicly accessible area*" as being any place open to any member of the public, for example a piazza, a shopping centre, a street, a market place, a train station or a public library.

of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications.

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale[16]:
    a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
    b. the volume of data and/or the range of different data items being processed;
    c. the duration, or permanence, of the data processing activity;
    d. the geographical extent of the processing activity.
6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject[17].
7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees , more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, *etc.*), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
8. Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, *etc*. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "*accordance with the achieved state of technological knowledge*" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.

[16] See the WP29 Guidelines on Data Protection Officer 16/EN WP 243.
[17] See explanation in the WP29 Opinion on Purpose limitation 13/EN WP 203, p.24.

9. When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract"* (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.

However, in some cases, **a data controller can consider that a processing meeting only one of these criteria requires a DPIA.**

The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:

Examples of processing	**Possible Relevant criteria**	**DPIA likely to be required?**
A hospital processing its patients' genetic and health data (hospital information system).	- Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects. - Data processed on a large-scale.	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	- Systematic monitoring. - Innovative use or applying technological or organisational solutions.	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, *etc*.	- Systematic monitoring. - Data concerning vulnerable data subjects.	
The gathering of public social media data for generating profiles.	- Evaluation or scoring. - Data processed on a large scale. - Matching or combining of datasets. - Sensitive data or data of a highly personal nature:	
An institution creating a national level credit rating or fraud database.	- Evaluation or scoring. - Automated decision making with legal or similar significant effect. - Prevents data subject from exercising a right or using a service or a contract. - Sensitive data or data of a highly personal nature:	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials	- Sensitive data. - Data concerning vulnerable data subjects. - Prevents data subjects from exercising a right or using a service or a contract.	

Examples of processing	Possible Relevant criteria	DPIA likely to be required?
A processing of "personal data from patients or clients by an individual physician, other health care professional or lawyer" (Recital 91).	- Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects.	No
An online magazine using a mailing list to send a generic daily digest to its subscribers.	- Data processed on a large scale.	
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.	- Evaluation or scoring.	

Conversely, a processing operation may correspond to the above mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.

In addition, as part of the accountability principle, every data controller "*shall maintain a record of processing activities under its responsibility*" including inter alia the purposes of processing, a description of the categories of data and recipients of the data and "*where possible, a general description of the technical and organisational security measures referred to in Article 32(1)*" (Article 30(1)) and must assess whether a high risk is likely, even if they ultimately decide not to carry out a DPIA.

Note: supervisory authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA to the European Data Protection Board (EDPB) (Article 35(4))[18]. The criteria set out above can help supervisory authorities to constitute such a list, with more specific content added in time if appropriate. For example, the processing of any type of biometric data or that of children could also be considered as relevant for the development of a list pursuant to article 35(4).

b) When isn't a DPIA required? When the processing is not "*likely to result in a high risk*", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required.

WP29 considers that a DPIA is not required in the following cases:

- **where the processing is not "*likely to result in a high risk to the rights and freedoms of natural persons*"** (Article 35(1));
- **when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out**. In such cases, results of DPIA for similar processing can be used (Article 35(1)[19]);

[18] In that context, "*the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union*" (Article 35(6)).

[19] "*A single assessment may address a set of similar processing operations that present similar high risks".*

- when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed[20] (see III.C);
- **where a processing operation,** pursuant to point (c) or (e) of article 6(1), **has a legal basis** in EU or Member State law, where the law regulates the specific processing operation **and where a DPIA has already been carried out** as part of the establishment of that legal basis (Article 35(10))[21], except if a Member state has stated it to be necessary to carry out a DPIA prior processing activities;
- **where the processing is included on the optional list (established by the supervisory authority) of processing operations** for which no DPIA is required (Article 35(5)). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorizations, compliance rules, *etc*. (e.g. in France, authorizations, exemptions, simplified rules, compliance packs…). In such cases, and subject to re-assessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with all the relevant requirements of the GDPR.

C. What about already existing processing operations? DPIAs are required in some circumstances.

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

A DPIA is not needed for processing operations that have been checked by a supervisory authority or the data protection official, in accordance with Article 20 of Directive 95/46/EC, and that are performed in a way that has not changed since the prior checking. Indeed, "*Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*" (recital 171).

Conversely, this means that any data processing whose conditions of implementation (scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the supervisory authority or the data protection official and which are likely to result in a high risk should be subject to a DPIA.

Moreover, a DPIA could be required after a change of the risks resulting from the processing operations[22], for example because a new technology has come into use or because personal data is

[20] "*Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed*" (recital 171).

[21] When a DPIA is carried out at the stage of the elaboration of the legislation providing a legal basis for a processing, it is likely to require a review before entry into operations, as the adopted legislation may differ from the proposal in ways that affect privacy and data protection issues. Moreover, there may not be sufficient technical details available regarding the actual processing at the time of adoption of the legislation, even if it was accompanied by a DPIA. In such cases, it may still be necessary to carry out a specific DPIA prior to carrying out the actual processing activities.

[22] In terms of the context, the data collected, purposes, functionalities, personal data processed, recipients, data combinations, risks (supporting assets, risk sources, potential impacts, threats, *etc*.), security measures and international transfers.

being used for a different purpose. Data processing operations can evolve quickly and new vulnerabilities can arise. Therefore, it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination. Each of these examples could be an element that leads to a change of the risk resulting from processing activity concerned.

Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

As a matter of good practice, **a DPIA should be continuously reviewed and regularly re-assessed.** Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.

D. How to carry out a DPIA?

a) At what moment should a DPIA be carried out? Prior to the processing.

The DPIA should be carried out "*prior to the processing*" (Articles 35(1) and 35(10), recitals 90 and 93)[23]. This is consistent with data protection by design and by default principles (Article 25 and recital 78). The DPIA should be seen as a tool for helping decision-making concerning the processing.

The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

The fact that the DPIA may need to be updated once the processing has actually started is not a valid reason for postponing or not carrying out a DPIA. The DPIA is an on-going process, especially where a processing operation is dynamic and subject to ongoing change. **Carrying out a DPIA is a continual process, not a one-time exercise**.

b) Who is obliged to carry out the DPIA? The controller, with the DPO and processors.

The controller is responsible for ensuring that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.

[23] Except when it is an already existing processing that has been prior checked by the Supervisory Authority, in which case the DPIA should be carried out before undergoing significant changes.

The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2)) and this advice, and the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c)). Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243.

If the processing is wholly or partly performed by a data processor, **the processor should assist the controller in carrying out the DPIA** and provide any necessary information (in line with Article 28(3)(f)).

The controller must "*seek the views of data subjects or their representatives*" (Article 35(9)), "*where appropriate*". The WP29 considers that:

- those views could be sought through a variety of means, depending on the context (e.g. a generic study related to the purpose and means of the processing operation, a question to the staff representatives, or usual surveys sent to the data controller's future customers) ensuring that the controller has a lawful basis for processing any personal data involved in seeking such views. Although it should be noted that consent to processing is obviously not a way for seeking the views of the data subjects;
- if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented;
- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable.

Finally, it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.:

- where specific business units may propose to carry out a DPIA, those units should then provide input to the DPIA and should be involved in the DPIA validation process;
- where appropriate, it is recommended to seek the advice from independent experts of different professions[24] (lawyers, IT experts, security experts, sociologists, ethics, *etc*.).
- the roles and responsibilities of the processors must be contractually defined; and the DPIA must be carried out with the processor's help, taking into account the nature of the processing and the information available to the processor (Article 28(3)(f));
- the Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context;
- the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.

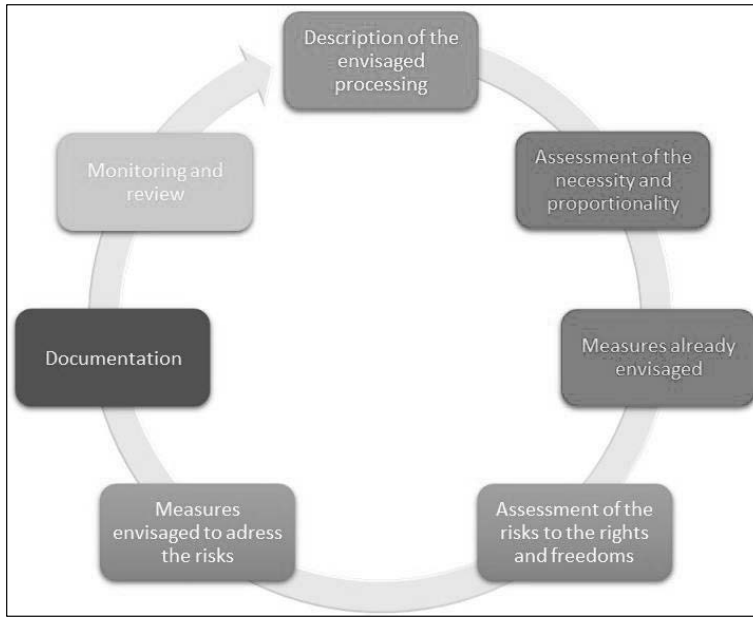
c) What is the methodology to carry out a DPIA? Different methodologies but common criteria.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

The GDPR sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- "*a description of the envisaged processing operations and the purposes of the processing*";
- "*an assessment of the necessity and proportionality of the processing*";
- "*an assessment of the risks to the rights and freedoms of data subjects*";
- "*the measures envisaged to:*
  - "*address the risks*";
  - "*demonstrate compliance with this Regulation*".

The following figure illustrates the generic iterative process for carrying out a DPIA[25]:



Compliance with a code of conduct (Article 40) has to be taken into account (Article 35(8)) when assessing the impact of a data processing operation. This can be useful to demonstrate that adequate measures have been chosen or put in place, provided that the code of conduct is appropriate to the processing operation. Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors (Article 42), as well as Binding Corporate Rules (BCR), should be taken into account as well.

[25] It should be underlined that the process depicted here is iterative: in practice, it is likely that each of the stages is revisited multiple times before the DPIA can be completed.

All the relevant requirements set out in the GDPR provide a broad, generic framework for designing and carrying out a DPIA. The practical implementation of a DPIA will depend on the requirements set out in the GDPR which may be supplemented with more detailed practical guidance. The DPIA implementation is therefore scalable. This means that even a small data controller can design and implement a DPIA that is suitable for their processing operations.

Recital 90 of the GDPR outlines a number of components of the DPIA which overlap with well-defined components of risk management (e.g. ISO 31000[26]). In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following processes, by:

- establishing the context: "*taking into account the nature, scope, context and purposes of the processing and the sources of the risk*";
- assessing the risks: "*assess the particular likelihood and severity of the high risk*";
- treating the risks: "*mitigating that risk*" and "*ensuring the protection of personal data*", and "*demonstrating compliance with this Regulation*".

Note: the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, as is the case in certain fields (e.g. societal security). Conversely, risk management in other fields (e.g. information security) is focused on the organization.

The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them.

Different methodologies (see Annex 1 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR. In order to allow these different approaches to exist, whilst allowing controllers to comply with the GDPR, common criteria have been identified (see Annex 2). They clarify the basic requirements of the Regulation, but provide enough scope for different forms of implementation. These criteria can be used to show that a particular DPIA methodology meets the standards required by the GDPR. **It is up to the data controller to choose a methodology, but this methodology should be compliant with the criteria provided in Annex 2**.

The WP29 encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectorial knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures). This means the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies or carrying out particular types of processing operation.

Finally, where necessary, *"the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operation"* (Article 35(11)[27]).

[26] Risk management processes: communication and consultation, establishing the context, risk assessment, risk treatment, monitoring and review (see terms and definitions, and table of content, in the ISO 31000 preview: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

[27] Article 35(10) explicitly excludes only the application of article 35 paragraphs 1 to 7.

d) Is there an obligation to publish the DPIA? No, but publishing a summary could foster trust, and the full DPIA must be communicated to the supervisory authority in case of prior consultation or if requested by the DPA.

Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.

The purpose of such a process would be to help foster trust in the controller's processing operations, and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA.

The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. In these circumstances, the published version could consist of just a summary of the DPIA's main findings, or even just a statement that a DPIA has been carried out.

Moreover, where a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be fully provided (Article 36(3)(e)). The supervisory authority may provide its advice[28], and will not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable in each Member State on public access to official documents.

E. <u>When shall the supervisory authority be consulted? When the residual risks are high.</u>

As explained above:

- a DPIA is required when a processing operation "*is likely to result in a high risk to the rights and freedoms of natural person*" (Article 35(1), see III.B.a). As an example, the processing of health data on a large scale is considered as likely to result in a high risk, and requires a DPIA;
- then, it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures[29] envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR (Article 35(7), see III.C.c). An example could be for the storage of personal data on laptop computers the use of appropriate technical and organisational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, *etc*.) in addition to existing policies (notice, consent, right of access, right to object, *etc*.).

In the laptop example above, if the risks have been considered as sufficiently reduced by the data controller and following the reading of Article 36(1) and recitals 84 and 94, the processing can proceed without consultation with the supervisory authority. It is in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remains high) that the data controller must consult the supervisory authority.

[28] Written advice to the controller is only necessary when the supervisory authority is of the opinion that the intended processing is not in line with the regulation as per Article 36(2).

[29] Including taking account of existing guidance from EDPB and supervisory authorities and taking account of the state of the art and the costs of implementation as prescribed by Article 35(1).

An example of an unacceptable high residual risk includes instances where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well-known vulnerability is not patched).

Whenever the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high), consultation with the supervisory authority is required[30].

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5)).

It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

IV. Conclusions and recommendations

DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processing operations. They are scalable and can take different forms, but the GDPR sets out the basic requirements of an effective DPIA. Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance.

Article 24(1) sets out the basic responsibility of the controller in terms of complying with the GDPR: "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*".

The DPIA is a key part of complying with the Regulation where high risk data processing is planned or is taking place. This means that data controllers should use the criteria set out in this document to determine whether or not a DPIA has to be carried out. Internal data controller policy could extend this list beyond the GDPR's legal requirements. This should result in greater trust and confidence of data subjects and other data controllers.

Where a likely high risk processing is planned, the data controller must:

- choose a DPIA methodology (examples given in Annex 1) that satisfies the criteria in Annex 2, or specify and implement a systematic DPIA process that:

[30] Note: "*pseudonymization and encryption of personal data*" (as well as data minimization, oversight mechanisms, *etc.*) are not necessarily appropriate measures. They are only examples. Appropriate measures depend on the context and the risks, specific to the processing operations.

  - is compliant with the criteria in Annex 2;
  - is integrated into existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture;
  - involves the appropriate interested parties and clearly define their responsibilities (controller, DPO, data subjects or their representatives, business, technical services, processors, information security officer, *etc*.);
- provide the DPIA report to the competent supervisory authority when required to do so;
- consult the supervisory authority when they have failed to determine sufficient measures to mitigate the high risks;
- periodically review the DPIA and the processing it assesses, at least when there is a change of the risk posed by processing the operation;
- document the decisions taken.

Annex 1 – Examples of existing EU DPIA frameworks

The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). Such a framework can be bespoke to the data controller or common across a particular industry. Previously published frameworks developed by EU DPAs and EU sector-specific frameworks include (but are not limited to):

Examples of EU generic frameworks:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Examples of EU sector-specific frameworks:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

An international standard will also provide guidelines for methodologies used for carrying out a DPIA (ISO/IEC 29134[34]).

---

[31] Unanimously and affirmatively acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016.

[32] See also :

- Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33] See also the Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

[34] ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

Annex 2 – Criteria for an acceptable DPIA

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
      - ☐ lawfulness of processing (Article 6);
      - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
      - ☐ limited storage duration (Article 5(1)(e));
    - ☐ measures contributing to the rights of the data subjects:
      - ☐ information provided to the data subject (Articles 12, 13 and 14);
      - ☐ right of access and to data portability (Articles 15 and 20);
      - ☐ right to rectification and to erasure (Articles 16, 17 and 19);
      - ☐ right to object and to restriction of processing (Article 18, 19 and 21);
      - ☐ relationships with processors (Article 28);
      - ☐ safeguards surrounding international transfer(s) (Chapter V);
      - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
  - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - ☐ risks sources are taken into account (recital 90);
    - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
    - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - ☐ likelihood and severity are estimated (recital 90);
  - ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- ☐ interested parties are involved:
  - ☐ the advice of the DPO is sought (Article 35(2));
  - ☐ the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).

NOTES

42

Information Commissioner's Office: Sample DPIA Template

Submitted by:
Lara Kehoe Hoffman
Netflix

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated, reduced or accepted	Low, medium or high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

NOTES

43

Hunton Andrews Kurth LLP,
Privacy & Information Security Law Blog:
Global Privacy and Cybersecurity Law
Updates and Analysis, European Data
Protection Board Issues Privacy Shield
Report (January 28, 2019)

Submitted by:
Lisa J. Sotto
Aaron P. Simpson
Hunton Andrews Kurth LLP

On January 22, 2019, the European Data Protection Board ("EDPB") issued a report on the Second Annual Review of the EU-U.S. Privacy Shield (the "Report"). Although not binding on EU or U.S. authorities, the Report provides guidance to regulators in both jurisdictions regarding implementation of the Privacy Shield and highlights the EDPB's ongoing concerns with regard to the Privacy Shield. We previously blogged about the European Commission's report on the second annual review of the Privacy Shield, and the joint statement of the European Commission and Department of Commerce regarding the second annual review.

In the Report, the EDPB praised certain actions and efforts undertaken by U.S. authorities and the European Commission to implement the Privacy Shield, including the following:

- Efforts by the Department of Commerce to adapt the initial certification process to minimize inconsistencies between the Department's Privacy Shield List and representations made by certifying organizations (in their privacy notices) regarding their participation in the Privacy Shield;
- Enforcement actions and other oversight measures taken by the Department of Commerce and Federal Trade Commission regarding compliance with the Privacy Shield; and
- Issuance of guidance for EU individuals on exercising their rights under the Privacy Shield, and for U.S. businesses to clarify the requirements of the Privacy Shield (g., the Department of Commerce's FAQs available on PrivacyShield.gov).

The Report identifies continuing concerns of the EDPB, including the following key areas:

- According to the EDPB, "a majority of companies' compliance with the substance of the Privacy Shield's principles remain unchecked." The EDPB indicated that the application of the Shield principles by certifying organizations has not yet been ascertained through oversight and enforcement action by U.S. authorities.
- With respect to the onward transfer principle, the EDPB suggested that U.S. authorities more closely monitor the implementation of this principle by certified entities, suggesting, for example, that the Department of Commerce exercise "its right to ask organizations to produce the contracts they have put in place with third countries' partners" to assess whether the contracts provide the required

safeguards and whether further guidance or action by the U.S. authorities is needed in this regard.

- The EDPB indicated that the re-certification process "needs to be further refined," noting that the Privacy Shield list contains outdated listings, leading to confusion for data subjects.
- The Report highlights the uncertainty surrounding the application of the Privacy Shield to HR data, noting that conflicting interpretations of the definition of HR data has led to uncertainty as to what protections are available.

In addition, the Report notes that the EDPB is still awaiting the appointment of a permanent independent Ombudsperson to oversee the Privacy Shield program in the U.S. Until such time as an appointment is made, the EDPB cannot determine whether the Ombudsperson "is vested with sufficient powers to remedy non-compliance" with the Privacy Shield.

HUNTON BRIEFING REFLECTS ON GDPR IMPLEMENTATION AND FUTURE CHALLENGES

January 28, 2019

On January 16, 2019, Hunton Andrews Kurth hosted a breakfast seminar in London, entitled "GDPR: Post Implementation Review." Bridget Treacy, Aaron Simpson and James Henderson from Hunton Andrews Kurth and Bojana Bellamy from the Centre for Information Policy Leadership ("CIPL") at Hunton Andrews Kurth discussed some of the challenges and successes companies encountered in implementing the EU General Data Protection Regulation (the "GDPR"), and also identified key data protection challenges that lie ahead. The Hunton team was joined by Neil Paterson, Group Data Protection Coordinator of TUI Group; Miles Briggs, Data Protection Officer of TUI UK & Ireland; and Vivienne Artz, Chief Privacy Officer at Refinitiv, who provided an in-house perspective on the GDPR.

The briefing provided an opportunity for companies (the "Companies") to reflect on their achievements so far and to benchmark their GDPR experiences ahead of Data Protection Day, which is on January 28, 2019. A main takeaway of the day was that building a business friendly privacy environment is an ongoing process that must be viewed from a global perspective.

We have summarized below some of the key discussion points from the seminar.

GDPR Implementation Insights

- **Generally Satisfied with Compliance**: While the Companies were reasonably satisfied with the bulk of their GDPR implementation work and are now engaged in fine-tuning their data protection compliance programs, the Companies recognized that a number of challenges remain.
- **Global Privacy Challenges**: Data Protection Officers are seeking to move their companies toward sustainable privacy programs that ensure GDPR compliance, yet also address global privacy challenges beyond the GDPR. The Companies view GDPR compliance as important, but not an end in itself, at least not given recent developments in other parts of the world, such as India, Brazil, etc. The Companies recognize privacy as the new normal, and are working to build efficient programs to address privacy challenges at an international level.
- **Maintaining a Culture of Privacy Awareness**: Maintaining and developing a culture of privacy awareness within their companies is a key concern for privacy leaders. Some business leaders viewed the GDPR as a completed task once the implementation date of May 25, 2018, had passed, rather than an ongoing responsibility; and privacy leaders have been working hard to correct this view.
- **Territorial Scope**: Many of the Companies have struggled to interpret the territorial scope of the GDPR. Insights from the European Data Protection Board's Guidelines on Territorial Scope (3/2018), published in November 2018, have helped to clarify the position on topics such as the location of the protected data subjects, the use of non-EU based processors and the nature of a non-EU processor's obligations.
- **Data Processing Agreements**: Implementing Article 28 requirements continues to challenge the Companies, with a broad range of positions being adopted when negotiating data processing agreements. Negotiating liability caps and exclusions can be complex, due in part to the risk of reopening broader liability and other contractual issues. It will likely take some time for market practice to evolve.
- **Increased Training and Tech-enabled Compliance Tools**: The Companies mentioned that, in the year ahead, conducting data protection training and awareness programs and rolling out

tech-enabled compliance tools (e.g., for DPIAs and DSARs) will play a key part in enabling ongoing compliance with the GDPR.

- **GDPR and Future Privacy Challenges**: The Companies stressed the difficulties encountered in interpreting and implementing GDPR obligations in the context of artificial intelligence, machine learning and the big data challenges of tomorrow. Companies will need to find innovative ways to accommodate big data while respecting data subject rights.

Regulatory Perspective

- **Increase in Complaints and Breach Reporting**: As expected, data protection authorities ("DPAs") have already been required to deal with a significant volume of complaints (on one report, 42,230 throughout the EU), and reports of data breaches (some 500 per week in the UK in the first few weeks after the GDPR took effect). Breach notifications across EU Member States have reached levels that are barely sustainable for most EU regulators. This is a consequence of the low notification threshold set by the GDPR, and of organizations adopting a very conservative approach towards notification. The ICO has reminded organizations that not all data breaches need to be reported. Other DPAs have a differing view, pointing to the need for more comprehensive guidance on this topic.
- **Inconsistency across Member States**: There are already examples of inconsistent approaches by EU DPAs in relation to the implementation of the GDPR framework. Perhaps the starkest example of this is the 21 separate DPIA frameworks adopted at a national level. Staffing levels between DPAs differ, and differences in enforcement strategy are also likely. It will take time for differences to be reconciled, and in some areas, they will remain. Just as companies require time to embed and fine tune their implementation of the GDPR, regulators will also require time to adjust to the new regulatory environment.

Future Challenges

- **Moving Beyond Local Compliance to Global Privacy Accountability**: Privacy frameworks are evolving and organizations face the challenge of moving their focus from local legal compliance to implementing a global operational privacy framework. The GDPR

is now viewed as a template by countries seeking to craft new privacy laws. It offers a major step forward towards an operational privacy framework, but global privacy accountability will remain a challenge.

- **Local Challenges**: Privacy leaders aspire to ensure that at every level of their organization, staff recognize the privacy issues raised by each decision, and assess the privacy risk for affected data subjects.
- **Future Challenges**: Major legal challenges highlighted by participants included Brexit, the e-Privacy Regulation and the likelihood of legal challenges under the GDPR.

CCPA: EMPLOYERS SHOULD CONSIDER IMPLICATIONS FOR EMPLOYEE BENEFIT PLANS

January 16, 2019

As we move closer to implementation of the California Consumer Privacy Act of 2018 ("CCPA"), companies should consider how the new law could affect their operations in multiple ways – including, for example, data collected through their employee benefit plans.

As we have previously reported, the CCPA applies broadly to any for-profit business that meets certain thresholds and that collects personal information regarding consumers. While use of the term "consumer" may suggest a particular type of relationship, the term is defined broadly to include any California resident – and as a result, in its current form the CCPA also will apply to information collected by covered businesses about their California employees. Whether the CCPA also applies to data collected about California residents under employee benefit plans of covered businesses will likely depend in part on the type of plan:

- ***Health Plans***. Following its amendment in September 2018, the CCPA includes an exemption for protected health information ("PHI") collected by a covered entity or business associate subject to the HIPAA privacy rules. Because employer-sponsored health plans are HIPAA-covered entities, any PHI held by a self-insured plan and subject to HIPAA will be outside the reach of the CCPA. The exemption also applies to PHI held by business associates, such as third-party administrators for health plans. However, certain other health-related information that is held by an employer outside of the

health plan – such as information related to disability benefits or sick leave – is not covered by this exemption.

- ***Retirement and other ERISA Plans***. The CCPA does not specifically address its application to benefit plans not covered by HIPAA. For plans that are subject to the Employee Retirement Income Security Act of 1974 ("ERISA"), such as 401(k) plans and other qualified retirement plans, it is possible that the CCPA could be preempted by ERISA – but unlike the health plan exemption, it is not clear from the statute.
    - In general, ERISA preempts state laws that govern a central matter of plan administration or that impermissibly interfere with nationally uniform plan administration. For example, in its 2016 decision in *Gobeille v. Liberty Mutual Insurance Company*, the U.S. Supreme Court held that ERISA preempted a Vermont law requiring various entities, including self-insured plans and third party administrators, to report payments relating to health care claims and other information regarding health care services.
    - The CCPA imposes new requirements regarding retention and deletion of personal information, and certain disclosures regarding use of personal information. Because reporting, disclosure and recordkeeping are key areas of regulation under ERISA, it is possible the law could be preempted on the basis that it impermissibly interferes with plan administration. In the absence of further guidance, however, it is not certain to what extent preemption would apply – and it is also possible that a court could find that ERISA preempts some aspects of the law but not others.
- ***Non-ERISA Benefits and Employment Practices***. Even if the CCPA is ultimately determined to be preempted in the context of ERISA plans, it will still apply to data collection by an employer in its capacity as an employer, as well as data related to benefits and policies not covered by ERISA. This includes information collected by an employer in connection with administering vacation, sick leave, paid time off or leaves of absence. Other benefits that are generally not subject to ERISA include health savings accounts, dependent care flexible spending accounts, many short-term disability plans and certain voluntary benefits.

The California State Legislature is expected to consider more changes to the CCPA in 2019 – so we may receive more guidance about the application of the law in the employment context. In the meantime, employers and benefit plan sponsors subject to the CCPA will want to consider how the new law could apply to their own benefit plans and the data of their plan participants and beneficiaries. Since many plans are administered by third party record-keepers, employers and plan sponsors may also want to reach out to their vendors to ask about any plans being put in place to comply with the CCPA.

MASSACHUSETTS AMENDS DATA BREACH LAW; IMPOSES ADDITIONAL REQUIREMENTS

January 14, 2019

On January 10, 2019, Massachusetts Governor Charlie Baker signed legislation amending the state's data breach law. The amendments take effect on April 11, 2019.

Key updates to Massachusetts's Data Breach Notification Act include the following:

- The required notice to the Massachusetts Attorney General and the Office of Consumer Affairs and Business Regulation will need to include additional information, including the types of personal information compromised, the person responsible for the breach (if known) and whether the entity maintains a written information security program. Under Massachusetts 201 CMR § 17.03, any entity that owns or licenses personal information about a Massachusetts resident is currently obligated to develop, implement and maintain a comprehensive written information security program that incorporates the prescriptive requirements contained in the regulation.
- If individuals' Social Security numbers are disclosed, or reasonably believed to have been disclosed, the company experiencing a breach must offer credit monitoring services at no cost for at least 18 months (42 months, if the company is a consumer reporting agency). Companies also must certify to the Massachusetts attorney general and the Director of the Office of Consumer Affairs and Business Regulation that their credit monitoring services are compliant with state law.

- The amended law explicitly prohibits a company from delaying notice to affected individuals on the basis that it has not determined the number of individuals affected. Rather, the entity must send out additional notices on a rolling basis, as necessary.
- If the company experiencing a breach is owned by a separate entity, the individual notice letter must specify "the name of the parent or affiliated corporation."
- Companies are prohibited from asking individuals to waive their right to a private action as a condition for receiving credit monitoring services.

CYBERSECURITY RULES FOR INSURANCE COMPANIES TO TAKE EFFECT IN SOUTH CAROLINA

January 2, 2019

New cybersecurity rules for insurance companies licensed in South Carolina are set to take effect in part on January 1, 2019. The new law is the first in the United States to be enacted based on the data security model law drafted by the National Association of Insurance Commissioners. The law requires licensed insurance companies to notify state insurance authorities of data breaches within 72 hours of confirming that nonpublic information in the company's (or a service provider's) system was "disrupted, misused, or accessed without authorization." The breach reporting requirement is in addition to notification obligations imposed under South Carolina's breach notification law and applies if the insurance company has a permanent location in the state or if the breach affects at least 250 South Carolina residents, among other criteria. The 72-hour notice requirement takes effect January 1, 2019.

Separately, effective July 1, 2019, the law requires insurance companies licensed in South Carolina to develop and implement a comprehensive, written cybersecurity program. Among other details, the program must be based on a company's own risk assessments and must include encryption of information in transit, regular testing of systems, and cybersecurity awareness training for employees. The law will also require insurance companies to "exercise due diligence" in choosing third-party service providers and to ensure that service providers have appropriate information safeguards in place no later than July 1, 2020.

AGREEMENT ON PROPOSAL FOR CYBERSECURITY ACT

December 20, 2018

The European Commission ("Commission"), the European Parliament ("Parliament") and the Council of the European Union reached an agreement earlier this month regarding changes to the Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification (the "Cybersecurity Act"). The agreement empowers the EU Cybersecurity Agency (known as European Union Agency for Network and Information and Security, or "ENISA") and introduce an EU-wide cybersecurity certification for services and devices.

Background

The Cybersecurity Act was introduced in a wide-ranging set of cybersecurity measures adopted by the Commission on September 13, 2017, and proposed as a priority of the Digital Single Market Strategy. The objective of these measures was to deal with cyber-attacks and build strong cybersecurity in the EU.

More Powers for ENISA

The Cybersecurity Act reinforces the ENISA's centrality to better support Member States when facing cybersecurity threats or attacks. The Cybersecurity Act grants more powers to and new tasks for ENISA, including:

- A permanent mandate. The initial temporary mandate was due to end in 2020 and is now replaced by a permanent mandate. More resources will also be allocated to ENISA to accomplish its tasks.
- To prepare the EU for a crisis response to major cyberattacks.
- To assist Member States in responding effectively to cyber-attacks with a greater cooperation and coordination at the EU level.

ENISA will also be recognized as an independent center of expertise that will promote awareness to citizens and businesses and that will assist the EU institutions and Member States in the development and implementation of policies.

Cybersecurity Certification Framework

The Cybersecurity Act also introduces an EU-wide cybersecurity certification framework to ensure that the products and services sold in the EU comply with EU cybersecurity standards. This a great step forward as it is the first internal market law that enhances the security of connected products, Internet of Things or critical infrastructure by implementing a single certificate.

The hope is that consumers will benefit from this new regulation as manufacturers provide detailed information on cybersecurity for certified products and services including guidance on installation, the period for security support and information for security updates. The Cybersecurity Act, in this view, will increase consumers' trust in products and services they choose to use as they will have warranties that these products and services are cyber secure.

Similarly, companies will also benefit from the Cybersecurity Act as they will save significant costs on certification. A one stop-shop cybersecurity certification means that companies and especially Small and Medium-sized Enterprises ("SMEs") will not need to apply for certificates in different countries but one certificate will be valid throughout the EU. Certification will no longer be perceived as a market-entry barrier for companies but as a competitive advantage. In addition, companies may certify their own products for a minimum level of cybersecurity.

Better Governance

To make future initiatives clearer and more transparent for industry, the Parliament requested that a Union rolling work program be a component of the cybersecurity certification framework's governance, and involved in setting the strategic priorities on future certification requirements.

Next Steps

The Parliament's Committee on Industry, Research and Energy and the Council of the European Union must still formally approve the proposed agreement. If approved, it will then be published in the EU Official Journal. The Cybersecurity Act will enter into force twenty days following that publication.

EDPB PUBLISHES GUIDELINES ON EXTRATERRITORIAL APPLICATION OF THE GDPR

November 27, 2018

On November 23, 2018, the European Data Protection Board ("EDPB") published its long-awaited draft guidelines on the extraterritorial application of the EU General Data Protection Regulation ("GDPR") (the "Guidelines"). To date, there has been a degree of uncertainty for organizations regarding the scope of the GDPR's application outside of the EU. While the Guidelines provide some clarity on this issue, questions will remain for non-EU controllers and processors. Importantly, these Guidelines are only in draft form and are open for consultation until January 18, 2019, which will give organizations an opportunity to provide comments and raise additional questions in an effort to obtain further clarification from the EDPB on these important scoping questions.

Under Article 3 of the GDPR, the law applies to organizations that process personal data in three circumstances:

1. When a controller or processor is established in the EU and processes personal data in the context of the activities of that establishment;
2. When a controller or processor is not established in the EU but processes personal data relating to the offering of goods or services to individuals in the EU; or
3. When a controller or processor is not established in the EU but monitors the behavior of individuals in the EU.

Given the extensive obligations imposed by the GDPR and the onerous enforcement regime, global organizations have been rightly focused on how their own data processing activities may (or may not) fit within the scope of Article 3. While the Guidelines do not resolve all of these questions, they do provide some clarity. We have summarized and assessed the key aspects of the Guidelines below.

- For controllers and processors that are located in the EU, the Guidelines reiterate that the GDPR applies to the processing of personal data by those EU establishments regarding all data subjects, regardless of their location or nationality. For example, the processing of personal data by a French controller relating to customers in the U.S. is subject to the GDPR. As a practical matter, this means that the GDPR will apply in full with respect to this processing, including with respect to data subject rights available under the GDPR, which

in this hypothetical would be conferred upon the controller's customers in the U.S.

- A non-EU controller that is not otherwise subject to the GDPR will not become subject to the GDPR merely because a data processor located in the EU processes personal data on its behalf. This reiterates the conventional interpretation of Article 3, as this non-EU controller would not be established in the EU, nor would it be offering goods or services to individuals in the EU or monitoring behavior in the EU on account of retaining an EU processor.
- If a controller subject to the GDPR uses a non-EU processor that is not otherwise subject to the GDPR, that processor will not become directly subject to the GDPR on account of this processing. Notably, the Guidelines state that "the existence of a relationship between a controller and a processor does not necessarily trigger the application of the GDPR to both, should one of these two entities not be established in the Union." Instead, the controller subject to the GDPR will need to execute an Article 28 agreement with the non-EU processor. As a practical matter, this means that, from a contractual perspective, the processor will be subject to many of the same substantive obligations imposed on processors subject to the GDPR. This also means, however, that breaches of these Article 28 contractual obligations by such processors will only be enforceable as breaches of contract, not as direct GDPR infringements.
- With regards to controllers or processors that are not established in the EU but process personal data relating to the offering of goods or services to individuals in the EU, the Guidelines confirm that the key factor for determining scope is whether the controller or processor intends to "target" individuals in the EU. The mere accessibility of a website from the EU, for example, is insufficient. The Guidelines provide a non-exhaustive list of nine factors that may indicate an intention to offer goods or services to individuals in the EU, including running marketing campaigns aimed at an EU audience, the use of EU-related domain names, the provision of dedicated contact telephone numbers for individuals in the EU, and the delivery of goods to locations in the EU.
- With regards to controllers or processors that are not established in the EU but monitor the behavior of individuals in the EU, the Guidelines acknowledge that unlike the "offer of goods or services" prong discussed above, the "monitoring" prong does not include an

"intention to target" criteria for purposes of determining application of the GDPR. The Guidelines do, however, provide clarity with respect to the "monitoring" prong by stating that "the EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as 'monitoring'." Rather, the EDPB states that "the use of the word 'monitoring' implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour within the EU." This is an important clarification, as it implies a degree of intentionality must be present with respect to the collection and reuse of personal data of individuals in the EU by organizations outside the EU for it to constitute cognizable "monitoring." Accordingly, a website based in the U.S. that is focused on the U.S. market does not necessarily fall within the scope of the GDPR simply on account of the fact that an individual in the EU visits the website and the website engages in automated data collection. For the GDPR to apply, the U.S. website would need to have a "specific purpose in mind" with respect to its collection and reuse of the EU visitor's personal data, which is unlikely for a business singularly focused on the U.S. market.

- The Guidelines recommend that Article 27 representatives should be located in the EU Member State in which the majority of data subjects whose personal data are processed are located. In addition, the Guidelines confirm that, in principle, enforcement action for non-compliance with the GDPR by the controller or processor could be initiated against the EU representative "in the same way as against controllers or processors," including the possibility of imposing administrative fines and penalties.

There was an expectation that the Guidelines would provide guidance related to how the restrictions on transfers of personal data outside the EU are intended to coexist with the extraterritorial application of the GDPR, but the draft did not address this issue directly. Once the consultation period ends on January 18, 2019, we expect the Guidelines to be published in final form by April 2019.

NOTES

Index

A

Artificial Intelligence and Data Protection in Tension
- capabilities, 1053–1055
- executive summary, 1051
- introduction, 1051–1053
- observations, 1065–1067
- public and private uses, 1055–1058
- tension with data protection, 1058–1065

B

Big Data, Privacy, Research, and De-Identification
- description, 1015–1019

Blockchain
- challenges and solutions for compliance with GDPR, 987–1002

BNA, Inc., Privacy & Security Law Report
- how-to guide to information security breaches, 529–533

C

California Consumer Privacy Act of 2018
- business obligations
  - prohibit the of sale of personal information, 154–156
  - respond to a request for information, 148–152
  - right of erasure, 152–154
- conflicts with other laws, 177
- consumer privacy fund, 176–177
- consumer's right
  - access to information, 144–146
  - right erasure, 146
  - sale of personal information, 146–147
- consumers' private right of action in case of security breach, 170–174
- content of privacy policy or policies, 158–160
- development, regulations and procedures, 174–175
- enforcement, injunctions and fines, 168–170
- entities subject, 131–134
- financial incentives, 156–157
- impact on retailers, 181–183
- important definitions, 142–144
- individuals protected, 134–136
- information protected, 136–142
- interaction with service providers and third parties, 166–168
- obligation to inform consumers of their rights, 160–162
- overview and background, 131
- response to a consumer's request, 164–165
- role of state attorney general, 176
- submission of requests, 162–164
- training obligations, 166
- waiver and work, 147–148

Cyber Crime Wave
- cyber insurance premium growth follows growing wave of cyber crime, 551–554

Cyber Property
- how much risk do you want to keep in-house, 593–597

Cybering Up for Your Safety
- 15-step program will help you recover from unsafe practices, 583–585, 587–588

Cybersecurity Legal Requirements for All Businesses
- appendix, 479–492
- data security, definition, 439–441
- duty to provide security, 441–442
  - come from, 442–449
  - defining "reasonable" security, 450–469
  - harbor for reasonable security, 472–475
  - nature of the legal obligation, 449–450
  - special rules for specific data elements, 469–470
  - special rules for specific security controls, 471–472

Cybersecurity Legal *(Cont'd)*
duty to warn of security breaches, 475–478
overview, 437–439

D

Data Protection Working Party
annex 1, examples of existing eu DPIA frameworks, 1099
annex 2, criteria for an acceptable DPIA, 1101
conclusions and recommendations, 1096–1097
introduction, 1081
regulation explained, 1083–1086
scope of the guidelines, 1081–1082
Data-Rich Contracting Post-GDPR
conclusion, 817
data and rights of data subject, 808–809
definitional matters, 805–806
description, 803–804
during and after negotiations and contract, 809–817
keep a historical context, 804–805
still rife with uncertainty, 806–808
Digital Health Regulatory Gaps
conclusion, 1039
dangers, non-regulation, 1037
digital health, 1029–1030
encouraging compliance, 1037–1039
introduction, 1029
legal and regulatory frameworks, 1031–1037
risks, 1030–1031
Discoverability of Witness Interviews in California
application, work product doctrine and the attorney-client privilege, 701–705
DPIA Template
sample, 1105–1111

E

EU General Data Protection Regulation
administrative provisions, 276–277
breach of security, 240–243
codes of conduct and certification, 247–249
consent, 218–222
consistency, 273–275
data protection impact assessment, 230–236
data protection officer, 243–247
data security, 239–240
delegated acts and implementing acts, 275
European Data Protection Board, 271–273
general rules, processing of information, 204–209
goal, 188–189
intent to create a uniform framework, 189–191
interpretation and implementation, 192–194
introduction, 187–188
notable enforcement actions, 277–281
obligations
of data controllers, 209–214
of data processors, 214–218
principal parties, 194–196
remedies, liabilities, and penalties, 256–263
rights of data subjects, 249–256
special categories of processing, 236–239
subject matter scope, 196–200
supervisory authority, 263–271
territorial scope, 200–204
transfer of personal data to third countries, 222–230

F

Faculty Bios
Aaron P. Simpson, 106
Adam Rivera, 100
Aimee Nolan, 96
Al Saikali, 104
Alan Charles Raul, 98–99
Alejandro Mosquera, 91
Alexandra Ross, 101
Amanda Katzenstein, 71
Andrew Sawyer, 105
Antony (Tony) P. Kim, 74–75

Aristedes Mahairas, 85
Christine E. Lyon, 84
Clark Russell, 103
D. Esther Chavez, 49
Darren Abernethy, 41
Dave Wong, 117
Deborah Hirschorn, 66
Derek Care, 46
Emily Yu, 122
Eric M. Friedberg, 60–61
Ericka Watson, 115
Erika Brown Lee, 79
Flora J. Garcia, 64
Francoise Gilbert, 37–38
Harvey Jang, 70
Hilary M. Wandall, 1-114
J. Andrew Heaton, 65
Jacob Springer, 109
Jason N. Smolanoff, 107
Jah-Juin "Jared" Ho, 67
James G. Snell, 108
Jennifer King, 76
Jody R. Westby, 116
John F. Hyland, 69
Jonathan D. Avila, 42
Jonathan Fox, 59
Joseph J. Lazzarotti, 77–78
Katherine L. Kettler, 73
Kathleen M. Porter, 97
Kathryn J. Fritz, 62–63
Keith Enright, 57
Kerry Childe, 50
Kirk Nahra, 94–95
Kumneger Emiru, 56
Lara Kehoe Hoffman, 68
Laura Juanes Micas, 88
Lesley Matty, 87
Lisa J. Sotto, 39
Lisa R. Lifshitz, 81
Lydia de la Torre, 52–53
Maneesha Mithal, 90
Margaret Keane, 72
Marianne Fogarty, 58
Marty Myers, 92–93
Matthew W. Van Hise, 111
Maureen A. Young, 121
Merri A. Baldwin, 43
Michele Lucan, 83
Michelle Visser, 113
Miriam Wugmeister, 119–120
Patrice Malloy, 86
Peter Lefkowitz, 80
Polina Zvyagina, 123
Rachel Roy, 102
Rebecca S. Eisner, 55
Robert Lord, 82
Ruth Hill Bro, 44–45
Ryan Vinelli, 112
Stephanie Driggers, 54
Stephen S. Wu, 118
Steven Chabinsky, 47–48
Steven M. Cooper, 51
Thomas J. Smedinghoff, 40
William E. Min, 89
Zoë Strickland, 110
Formal Opinion No. 2012-183
attorney disclose client confidences, 733–737

G

GDPR
able to benefit from the one-stop-shop mechanism, 309
are you subject, 297
current contracts, clients need to be amended, 306
data subject requests, 285
data transfers, 285–286
definition, 295–296
enforcement, 286
example, sub-contracting contractual clauses, 312–319
fine imposed by restricted committee and its publicity, 290–291
handling of complaints by CNIL, 287–288
my obligations, not established in eu, 310
my role event of a data breach, 307
my role regard to the impact assessment, 308
primary change, 298
risks, if i do not comply with my obligations, 311
use another processor, my obligations, 305

GDPR *(Cont'd)*
violations observed by restricted committee, 288–290
where should you start, 302–304
your obligations, 299–301
Global Privacy and Cybersecurity Law Updates and Analysis
agreement on proposal for Cybersecurity Act, 1123–1124
CCPA, 1119–1121
cybersecurity rules, insurance companies, 1122
description, 1115–1116
EDPB publishes guidelines, 1125–1127
Hunton briefing reflects, 1116–1119
imposes additional requirements, 1121–1122

H

Health Care Privacy and Security Issues to Watch in 2019
top five issues, 1043–1045

I

Inside Job
consider the range of attacks committed by employees or trusted insiders, 559–562
Internet of Things
insurance coverage, related risks, 497–514

L

Latest Insights from Privacy and Data Security Regulators
get smart on data protection training, 613–627
lawyers' legal obligations to provide data security, 629–665
Legal and Business Issues in AI, Big Data and IoT
practical checklist, 941–952
Less Attractive to Cyber Enforcement
tips from the trenches, 781–799
Litigation Risks
mitigate litigation risks associated with data security and cyber defense, 763–776

M

Maintaining Privilege Over an Internal Investigation
conclusion, 728
introduction, 709
investigation
beginning, 710–715
end, 723–728
middle, 715–722
Managing Vendor Risks in a Changing Regulatory Landscape
appendix A, ten foundational tips for successful oversight of third party service providers, 837–846
appendix B, top tips for controlling privacy and security risks in third party service arrangements, 847–858
appendix C, top ten tips for controlling privacy and cybersecurity risks in third party service provider transactions, 859–861
description, 821–823
2019 top ten tips, 823–835
Mayer Brown Cybersecurity and Data Privacy Update
California enacts first state law targeting iot cybersecurity, 909–911
5 considerations, New York cybersecurity regulations, 912–915
cybersecurity data privacy, 871–892
DOJ releases updated cyber incident response guidance, 904–908
ePrivacy Regulation, 922–924
EU cyber threat landscape and outlook, 867–87
international developments, 925–930
keeping it private, 893–898
top tips, 899–903
what you need to know, 916–921

Moving Toward a New Health Care Privacy Paradigm
description, 1007–1011

N

New York Attorney General, Press Release
$148 million settlement with Uber over 2016 data breach, 675–678
$575,000 settlement with EmblemHealth after data breach exposed over 80,000 social security numbers, 669–671
COPPA settlement with Oath – formerly AOL – for violating children's privacy, 683–688
five companies whose mobile apps failed to secure user information transmitted over the internet, 693–696

P

Pratt's Privacy & Security Law Report
dealmakers ignore cyber risks at their own peril, 541–547
Preparing for New Cyber Threats
make sure you've got a comprehensive and tested plan, 601–604
Privacy and Data Security Due Diligence in M&A Transactions
Hunton Andrews Kurth client alert, 935–936
Privacy and Security Challenges of Advanced Technologies
conclusions, 982–983
introduction, 959–961
overseeing, managing, and improving, 961–973
privacy issues, 973–979
security issues, 979–982
Privacy and Security Developments in the Workplace
key steps to consider, data collected in investigations, 757–758
privacy and security laws affecting investigations, 741–757
Privacy Laws Around the World
Africa
Angola, 378–379
Bahrain, 379–380
Benin, 380–381
Burkina Faso, 381–382
Cape Verde, 382–383
Chad, 383–384
Cote D'Ivoire, 384–386
Equatorial Guinea, 386
Gabon, 387–389
Ghana, 389–390
introduction, 377
Israel, 390–392
Madagascar, 393
Mali, 394
Mauritius, 395
Morocco, 396
overview, 377
Qatar, 397–398
Senegal, 398–399
Seychelles, 399
South Africa, 399–400
Tunisia, 401
United Arab Emirates, 401–403
Americas
Antigua & Barbuda, 325
Argentina, 325–327
Aruba, 327–328
Bahamas, 328–329
Bermuda, 329–330
Brazil, 330–331
Canada, 331–332
Cayman Islands, 332–333
Chile, 333
Colombia, 334–335
Costa Rica, 335–336
Curacao, 337
Dominican Republic, 338–339
introduction, 323–324
Mexico, 339–340
Nicaragua, 341–342
overview, 324
Peru, 342–343
St. Maarten, 344
Uruguay, 344–347
Asia
Australia, 350–353
China, 353–355
Hong Kong, 355–356

Privacy Laws in the Western *(Cont'd)*
India, 357–359
introduction, 349–350
Japan, 359–362
Kazakhstan, 362–363
Kyrgyzstan, 363–364
Macao, 364
Malaysia, 364–366
New Zealand, 366–367
overview, 350
Philippines, 367–370
Singapore, 370–371
South Korea, 371–373
Taiwan, 373–374
Turkmenistan, 374–375
Europe and Eurasia
Albania, 406–407
Andorra, 408
Armenia, 409–410
Azerbaijan, 410–412
Belarus, 412–413
Bosnia and Herzegovina, 413–414
Georgia, 415
introduction, 405
Kosovo, 416–417
Macedonia, 417–418
Moldova, 418–419
Monaco, 419–420
Montenegro, 420–421
overview, 405–406
Russia, 421–423
San Marino, 424–425
Serbia, 425–426
Turkey, 426–427
Ukraine, 428–430
Program Schedule
beyond GDPR - privacy and data security compliance around the world, 16
complying with the California Consumer Privacy Act and other US privacy developments, 15
cybersecurity attacks: a survival guide, 17
cybersecurity readiness: addressing compliance risk, 16
ethical issues for privacy and data security professionals, 18
GDPR: one year later, 15
internal investigations – balancing employees privacy rights and company's goals and obligations, 18
the latest insights from privacy and data security regulators, 17
mitigating litigation risk: lessons learned from the trenches, 18
the privacy and security challenges of new technologies, 19
the protectors: CPOs, CISOs and the problem of compliance overload, 20
vendor management: ensuring compliance with privacy and cybersecurity requirements, 19
Public Company Cybersecurity Disclosure
new guidance, 519–525

S

Spreading Cyber Around
cyber coverage is popping up in multiple places, 575–579
Starving Your IT Budget
your failure to upgrade means your luck may be over, 567–571