

**Intellectual Property  
Course Handbook Series**

# **TechLaw Institute 2017: The Digital Evolution**

**Co-Chairs  
Philip Blum  
Marc S. Roth  
James G. Snell**

INTELLECTUAL PROPERTY  
Course Handbook Series  
Number G-1312

# TechLaw Institute 2017: The Digital Evolution

*Co-Chairs*  
Philip Blum  
Marc S. Roth  
James G. Snell

To order this book, call (800) 260-4PLI or fax us at (800) 321-0093. Ask our Customer Service Department for PLI Order Number 184792, Dept. BAV5.

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

Copyright © 2017 by Practising Law Institute. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of Practising Law Institute. 978-1-4024-2864-7

## **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.

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, Discover PLUS. For more information, visit <http://discover.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  
TECHLAW INSTITUTE 2017: THE DIGITAL EVOLUTION  
San Francisco and Live Webcast, March 6–7, 2017  
New York City, March 29–30

CONTENTS:

PROGRAM SCHEDULE .....	9
FACULTY BIOS .....	23
1. Emerging, Disruptive and Sharing Technologies: What Is the Sharing Economy and Where Is It Going? (December 10, 2016) .....	53
John C. Yates <i>Morris, Manning &amp; Martin LLP</i>	
2. The Virtual Workplace (December 9, 2016) .....	73
Joseph J. Lazzarotti <i>Jackson Lewis P.C.</i>	
3. Cloud Computing, SaaS and Outsourcing .....	115
Keith Larney Bonnie Yeomans <i>CA Technologies</i> Michelle Perez <i>Interpublic Group</i>	
4. Hot Issues in Tech Law Litigation .....	123
Philip Blum <i>CA Technologies</i> Manas Mohapatra <i>Twitter</i> Tyler Newby <i>Fenwick &amp; West LLP</i>	
5. Brief of <i>Amici Curiae</i> , Federal Law Enforcement Officers Association, Association of Prosecuting Attorneys, Inc., and National Sheriffs' Association in Support of the Government, <i>In re Apple v. FBI</i> , No. CM 16-10-SP (E.D. Cal. 2016) .....	145
Submitted by: Joseph V. DeMarco <i>DeVore &amp; DeMarco LLP</i>	

6.	<i>U.S. v. Knowles</i> , No. 16 Cr. 005 (PAE) (S.D.N.Y 2016).....	167
a.	Complaint.....	169
b.	Consent Preliminary Order of Forfeiture as to Specific Property/Money Judgment.....	185
c.	Letter in Response to Order of the Court.....	195
d.	Order.....	197
	Submitted by: Joseph V. DeMarco <i>DeVore &amp; DeMarco LLP</i>	
7.	The Use of Cloud Computing, Mobile Devices and Social Media in the Practice of Law (December 9, 2016).....	199
	Pamela A. Bresnahan <i>Vorys, Sater, Seymour and Pease LLP</i> Lucian T. Pera <i>Adams and Reese LLP</i>	
8.	Summary of 2016 Internet of Things Cases (January 2017).....	223
	James G. Snell Christian Lee <i>Perkins Coie LLP</i>	
9.	President’s Council of Advisors on Science and Technology, Report to the President—Big Data and Privacy: A Technological Perspective (May 2014) .....	239
	Submitted by: Christin S. McMeley <i>Davis Wright Tremaine LLP</i>	
10.	The White House, Interim Progress Report, Big Data: Seizing Opportunities, Preserving Values (February 2015) .....	321
	Submitted by: Christin McMeley <i>Davis Wright Tremaine LLP</i> Noga Rosenthal <i>Epsilon/Conversant</i>	
11.	Julie Brill, Commissioner, U.S. Federal Trade Commission, Speech, Keynote Address Before the 23rd Computers Freedom and Privacy Conference (June 26, 2013).....	335
	Submitted by: Noga Rosenthal <i>Epsilon/Conversant</i>	

12. Digital Advertising Alliance, Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (November 2015) .....	351
Submitted by: Noga Rosenthal <i>Epsilon/Conversant</i>	
13. U.S. Federal Trade Commission, Press Release, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (February 7, 2012).....	363
Submitted by: Noga Rosenthal <i>Epsilon/Conversant</i>	
14. U.S. Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (January 2016) .....	369
Submitted by: Noga Rosenthal <i>Epsilon/Conversant</i>	
15. Article 29 Data Protection Working Party, European Commission, Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU (September 16, 2014) .....	423
Submitted by: Noga Rosenthal <i>Epsilon/Conversant</i>	
16. Manatt, Phelps & Phillips, LLP, Advertising Law Newsletter (January–November 2016) .....	431
Submitted by: Marc S. Roth <i>Manatt, Phelps &amp; Phillips, LLP</i>	
INDEX .....	471

Program Attorney: Krista M. Gundersen



# Program Schedule



## **TechLaw Institute 2017: The Digital Evolution**

San Francisco and Live Webcast, [www.pli.edu](http://www.pli.edu), March 6-7, 2017

New York City, March 29-30

### **Day One – Program Schedule (9:00 a.m. – 5:00 p.m.)**

*Morning Session: 9:00 a.m. – 12:30 p.m.*

#### **9:00 a.m.            Introductory Remarks**

*SF & WEB:            Marc S. Roth, James G. Snell*

*NYC:                  Philip Blum, Marc S. Roth, James G. Snell*

#### **9:15 a.m.            Emerging, Disruptive, and Sharing Technologies**

- The shared economy and related legal issues
- New technologies that challenge existing business models and raise new legal issues
- Emerging issues in the mobile and IoT markets
- Regulatory and compliance issues

*SF & WEB:            Michele C. Lee, Keith Yandell, John C. Yates*

*NYC:                  John C. Yates*

#### **10:15 a.m.           The Virtual Workplace**

- Home networks and BYOD
- Compliance and employee monitoring
- Cloud computing issues
- Labor and employment considerations

*SF & WEB:            Esra A. Hudson, Scott Maples*

*NYC:                  Robert H. Cohen, Joseph J. Lazzarotti*

*11:15 a.m.           Networking Break*



**11:30 a.m.**

**Cloud Computing, SaaS, and Outsourcing**

- Overview of cloud offerings and comparison to outsourcing
- Benefits and risks of the cloud
- Laws that may apply to the vendor or the customer
- Contract issues – what's negotiable?

*SF & WEB:*

*Keith Larney*

*NYC:*

*Michelle Perez, Bonnie Yeomans*

*12:30 p.m.*

*Lunch*

*Afternoon Session: 1:45 p.m. – 5:00n p.m.*

**1:45 p.m.**

**Hot Topics in Tech Law Litigation**

- Enforceability of arbitration clauses
- Status of class certification decisions
- International discovery issues and protecting privilege
- Best practices for risk minimization

*SF & WEB:*

*Manas Mohapetra, Tyler G. Newby*

*NYC:*

*Philip Blum*

**2:45 p.m.**

**Cybersecurity, Hacking, and Data Breach**

- Data breaches: not if, but when
- In the aftermath of Target, what are leading companies doing to prevent hacks?
- Top 5 things you must do if you are hacked
- Foreign hackers and U.S. Law Enforcement

*SF & WEB:*

*Joseph V. DeMarco and Panel*

*NYC:*

*Joseph V. DeMarco and Panel*

*3:45 p.m.*

*Networking Break*

**4:00 p.m.**

**Evolving Legal Ethics: Portable Devices, the Cloud, and Social Media**

- Managing ethical risks of operating in the cloud
- Mobile devices and apps: protecting client confidentiality and minimizing risk
- Social media: latest developments in understanding and managing ethical concerns, including managing AVVO, LinkedIn and Google reviews
- Cybersecurity: the ethics and liability of protecting client confidences
- Risk management issues involving operating in the cloud

*SF, NYC, & WEB: Pamela A. Bresnahan, Lucian T. Pera*

## **Day Two – Program Schedule (9:00 a.m. – 12:15 p.m.)**

*Morning Session: 9:00 a.m. – 12:15 p.m.*

### **9:00 a.m.      The Internet of Things and the Wired Life**

- The Smart Home
- The Connected Car
- Wearable tech and the quantified self
- Eco-tech and smart infrastructure

*SF & WEB:      James G. Snell*

*NYC:             James G. Snell*

### **10:00 a.m.      Emerging Issues in Big Data and Analytics**

- What is Big Data? How it's used, how it's regulated, and the risks presented
- What laws apply and what are the risks and benefits of Big Data?
- What issues are most important to consider when collecting and retaining Big Data?
- How have webscraping and webcrawling technologies impacted data collection?
- Beyond PII – Predictive and cross device targeting

*SF & Web:      Moderator:      Christin S. McMeley*  
*Panelists:      Laura Berger, Martin J. Collins,*  
*Tristan Ostrowski, Alison Pepper*

*NYC:             Moderator:      Christin S. McMeley*  
*Panelists:      William Efron, Noga Rosenthal*

*11:00 a.m.      Networking Break*

**11:15 a.m.**

**Reaching Consumers in a Digital World:  
Marketing, Advertising, and Social Media**

- How has technology impacted how companies “speak” to consumers?
- How are advertisers using social media to reach consumers?
- What are the top concerns of consumer protection regulators?
- How native advertising is changing the digital advertising landscape

*SF, NYC, & WEB: Tsan Abrahamson, Marc S. Roth*

## **SAN FRANCISCO**

### **Co-Chairs:**

#### **Marc S. Roth**

Manatt, Phelps, & Phillips, LLP  
New York City

#### **James G. Snell**

Perkins Coie LLP  
Palo Alto

### **Faculty:**

#### **Tsan Abrahamson**

Cobalt LLP  
Berkeley, California

#### **Laura Berger**

Attorney, Division of Privacy and Identity Protection  
Federal Trade Commission  
San Francisco

#### **Pamela A. Bresnahan**

Vorys, Sater, Seymour and Pease LLP  
Washington, D.C.

#### **Martin J. Collins**

QuinStreet  
Foster City, California

#### **Joseph V. DeMarco**

DeVore & DeMarco LLP  
New York City

**Esra A. Hudson**

Manatt, Phelps & Phillips, LLP  
Costa Mesa, California

**Keith Larney**

Vice President and Managing Assistant General Counsel  
CA Technologies  
Islandia, New York

**Michele C. Lee**

Associate Director, Litigation and Competition  
Twitter  
San Francisco

**Scott Maples**

Former Vice President, General Counsel & Corporate Secretary  
Ruckus Wireless, Inc.  
Sunnyvale, California

**Christin S. McMeley**

Davis Wright Tremaine LLP  
New York City

**Manas Mohapatra**

Legal Director, Products  
Twitter  
San Francisco

**Tyler G. Newby**

Fenwick & West LLP  
San Francisco

**Tristan Ostrowski**

Senior Product Counsel (Android) and Legal Manager (Core Platforms)

Google

Mountain View, California

**Alison Pepper**

Former Assistant General Counsel & Senior Director of Public Policy

Internet Advertising Bureau

San Francisco

**Lucian T. Pera**

Adams and Reese LLP

Memphis

**John C. Yates**

Morris, Manning & Martin, LLP

Atlanta



## **NEW YORK CITY**

### **Co-Chairs:**

#### **Philip Blum**

Vice President, Senior Counsel  
CA Technologies  
Islandia, New York

#### **Marc S. Roth**

Manatt, Phelps, & Phillips, LLP  
New York City

#### **James G. Snell**

Perkins Coie LLP  
Palo Alto

### **Faculty:**

#### **Tsan Abrahamson**

Cobalt LLP  
Berkeley, California

#### **Pamela A. Bresnahan**

Vorys, Sater, Seymour and Pease LLP  
Washington, D.C.

#### **Robert H. Cohen**

Associate General Counsel  
Omnicom Group Inc.  
New York City

#### **Joseph V. DeMarco**

DeVore & DeMarco LLP  
New York City

**William Efron**

Director, Northeast Region  
Federal Trade Commission  
New York City

**Joseph J. Lazzarotti**

Jackson Lewis P.C.  
Morristown, New Jersey

**Christin S. McMeley**

Davis Wright Tremaine LLP  
New York City

**Lucian T. Pera**

Adams and Reese LLP  
Memphis

**Michelle Perez**

Assistant General Counsel Privacy  
Interpublic Group  
New York City

**Noga Rosenthal**

Chief Privacy Officer  
Epsilon/Conversant  
New York City

**John C. Yates**

Morris, Manning & Martin, LLP  
Atlanta

**Bonnie Yeomans**

VP, Privacy Officer, Regulatory Compliance Lawyer  
CA Technologies  
Islandia, New York



## **Faculty Bios**



## **Philip L. Blum**



Phil is currently a Vice-President at CA Technologies, a global provider of IT management software and solutions. CA Technologies, a publicly-traded company with more than 11,000 employees, is more than 40 years old and has offices in dozens of countries. As an in-house attorney for CA Technologies, Phil helps oversee and manage the company's global litigation. Phil is based in the company's Islandia, Long Island office.

Prior to joining CA Technologies in 2014, Phil was a Litigation Partner at Bingham McCutchen LLP. Prior to joining Bingham, Phil was an associate at Brown, Rayman, Millstein, Felder & Steiner LLP.

Phil's main area of focus is litigation, and includes offensive and defensive patent litigation, commercial, employment, and licensing matters, to name a few areas.

Phil received his J.D. from the Hofstra University School of Law in 1999, and his B.A. from the University of Maryland at College Park.



**Marc Roth** is a partner in the Media, Technology and Advertising division of Manatt, Phelps & Phillips, LLP and Co-Chair of the TCPA Compliance and Class Action Defense Group, resident in the firm's New York office. Marc has over 25 years of experience in consumer advertising and marketing law, having served at the Federal Trade Commission upon graduating law school and most recently as chief compliance counsel for a Time Warner company, before joining Manatt. He is ranked by Chambers as a leading U.S. lawyer for his Advertising Transactional work.

Clients ranging from Fortune 100 and 500 companies to start-up firms turn to Marc for his expertise in privacy, social media, telemarketing, claim substantiation, continuity and negative option marketing, and loyalty programs. He also counsels clients on various transactional matters, and guides them through federal and state government investigations. He frequently speaks and writes about privacy, social media and telemarketing issues.

Marc has decades of experience counseling clients on privacy matters, including drafting and amending online and offline privacy policies and advising on how data may be collected, shared and used in partner marketing arrangements. He advises on laws governing data use and security, including the Children's Online Privacy Protection Act, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Fair and Accurate Credit Transactions Act, Video Privacy Protection Act, HIPAA, CAN-SPAM Act and the E.U. Data Protection Directive. He has served as faculty and chairperson at legal and business privacy conferences and is often called upon to assist leading industry trade associations in preparing comments on FTC privacy-related rulemakings.

In the marketing arena, Marc counsels clients on developing and managing telemarketing and e-mail campaigns in compliance with the Telemarketing Sales Rule, the Telephone Consumer Protection Act, CAN –SPAM, and applicable state laws. He advises companies on how to develop and manage free trial, negative option and continuity marketing programs in compliance with all applicable laws, regulations and credit card processing rules. Marc also counsels clients on conducting marketing campaigns conducted through online social media networks such as Facebook, Twitter, Instagram, and others.

Last, Marc represents clients before federal and state regulatory authorities by responding to complaints, inquiries, investigations, subpoenas and civil investigative demands, and negotiating settlements with such bodies.

## Professional Biography



JAMES G. SNELL | PARTNER

PALO ALTO, CA  
3150 Porter Drive  
Palo Alto, CA USA  
+1.650.838.4367  
JSnell@perkinscoie.com

---

**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 patent litigation, Internet and privacy issues, trade secret matters, matters involving unfair competition claims under California Business and Professions Code section 17200, false advertising, and class actions.**

**Jim is a Certified Information Privacy Professional (CIPP) as designated by the International Association of Privacy Professionals (IAPP) and a co-chair of the IAPP's KnowledgeNet program.**



## Tsan Abrahamson

Tsan Abrahamson's practice focuses on strategic counseling in the areas of social media, sweepstakes, intellectual property, advertising, trademark clearance, trademark and copyright prosecution, licensing, and other business transactions. She also manages the adverse proceedings practice at the U.S. Patent and Trademark Office Trademark Trial and Appeal Board.

Tsan has an extensive practice in the area of marketing promotions, including social media promotions, such as on Facebook and Twitter, gift card and gift certificate marketing, print and online sweepstakes, contests, give-aways, warranties, rebates, and coupon promotions. She also advises on corresponding privacy issues related thereto.

Tsan's advertising practice includes working with regulatory agencies to comply with federal guidelines, including new FTC guidelines regarding affiliate marketing, CAN-SPAM, and the Deceptive Mail Prevention and Enforcement Act. She also advises on ad campaigns, including script review, storyboard clearance, and network media placement.

Tsan also has special expertise in children's marketing issues, including promotions and claim substantiation, COPPA compliance, and advertising to children in print and television media. She has been a SuperLawyer since 2009, and is in Who's Who Legal for her expertise in Internet and E-commerce matters. She was inducted into the American Law Institute in 2007.

In addition to her advertising and promotions work, Tsan has successfully prosecuted and defended thousands of trademarks with the U.S. Patent and Trademark Office and internationally, including difficult sound and sensory marks and design marks. She has registered hundreds of copyrights at the U.S. Copyright Office and overseas.

Tsan's professional affiliations include the International Trademark Association, the Brand Activation Association, and the American Bar Association. She is an adjunct professor of law at USF School of Law.

Prior to Cobalt LLP, Tsan was worldwide intellectual property and licensing counsel for LeapFrog Enterprises, Inc., She also practiced for 7 years with the San Francisco firm of Cooley Godward Kronish (formerly Cooley Godward), where she represented video game makers, online auction houses, pharmaceutical companies, and numerous other large companies. Tsan also spent 8 years as a chef.

Tsan completed her undergraduate work at Dartmouth College, and received both her JD and MBA from the UCLA School of Law and The Anderson Graduate School of Management, respectively. She is recognized by Strathmore's Who's Who for leadership and achievement in the law, and has been selected as a California Super Lawyer.

**Laura D. Berger** is an attorney in the Division of Privacy and Identity Protection at the Federal Trade Commission. She enforces federal laws that protect consumer privacy. Recently, her law enforcement work has focused on the privacy and security standards applicable to social media and to the Internet of Things. She also has worked on the agency's efforts to educate app developers about privacy, including the recent guide "Marketing Your Mobile App: Get it Right from the Start." In addition, she was author of the Commission's Safeguards Rule. She received a B.A. from Tulane University and a J.D. from the University of Michigan Law School. She works from the FTC's Regional Office in San Francisco.

- Pamela A. Bresnahan
- Vorys, Sater, Seymour and Pease LLP
- 

Pam is a partner in the Vorys Washington, D.C. office and is the Chair of the litigation practice group in that office. She serves as trial and appellate counsel in business and commercial litigation matters, with an emphasis on professional liability, errors and omissions and coverage litigation. She represents lawyers, financial institutions, broker/dealers, financial professionals, directors and officers, technology professionals, fiduciaries, insurers and other professionals. Pam serves as coverage and litigation counsel for insurers issuing errors and omissions policies. She represents businesses and individuals in securities, technology, intellectual property and other corporate litigation. She advises law firms and lawyers on management, ethics and risk prevention issues. Pam is a Fellow of the American College of Trial Lawyers and has been named in *Best Lawyers in America* in the areas of professional liability, professional responsibility, commercial litigation and bet-the-company litigation. Pam is a member of the ABA Board of Governors. She is admitted to practice in Maryland, the District of Columbia, New York, California and Illinois.

## **Robert H. Cohen**

**Position/Title:** Associate General Counsel

**Firm or Place of Business:** Omnicom Group Inc.

**Address:** 437 Madison Avenue, New York, NY  
10022

**Phone:** (212) 415-3721

**Fax:** (212) 415-3470

**E-Mail:** Robert.Cohen@omnicomgroup.com

**Primary Areas of Practice:** Labor &  
Employment/Litigation

**Law School/**

**Graduate School:** Fordham University School of Law

### **Work History:**

Robert Cohen has over 17 years of legal experience representing employers in all facets of labor and employment law. He joined Omnicom Group Inc. in August 2005 as Assistant General Counsel, Labor and Employment. In 2010, Robert also assumed responsibility for general litigation. Prior to joining Omnicom he was a Partner at Davis & Gilbert and an associate both at Davis & Gilbert and Proskauer Rose.

Currently, Robert's primary responsibilities include ensuring compliance with the various federal, state and local labor and

employment laws for all Omnicom companies. He also oversees all litigation involving Omnicom companies, including discrimination and wage and hour cases. While concentrating on the United States, Robert also has responsibility for worldwide labor and employment compliance. He has a JD from Fordham University School of Law and a Bachelor's degree in Industrial Labor Relations from Cornell University.

Marty Collins is the SVP of Corporate Development, Legal & Compliance at QuinStreet. Prior to joining QuinStreet Mr. Collins served as Vice President of Corporate Development at Bloom Energy, a distributed energy provider. Prior to that, Mr. Collins was the General Counsel and head of internal audit at Novellus Systems. He was also previously in charge of M&A and corporate and securities matters for Oracle Corporation's legal department. Mr. Collins received his law degree from Georgetown and his B.A. from Williams College.

**Joseph V. DeMarco** is a partner at DeVore & DeMarco LLP where he specializes in counseling clients on complex litigation and investigation issues involving a range of subjects including fraud and securities laws violations, information privacy and security, theft of intellectual property, and computer intrusions. His years of experience in private practice and in government handling the most difficult cybercrime investigations handled by the United States Attorney's Office have made him one of the nation's leading experts on white collar crime and the law relating to emerging technologies.

From 1997 to 2007, Mr. DeMarco served an Assistant United States Attorney for the Southern District of New York, where he prosecuted a wide range of white collar crimes and founded and headed the Computer Hacking and Intellectual Property (CHIPs) Program, a group of five prosecutors dedicated to investigating and prosecuting violations of federal cybercrime laws and intellectual property offenses, encompassing all forms of criminal activity affecting e-commerce.

Since 2002, Mr. DeMarco has served as an Adjunct Professor at Columbia Law School, where he teaches the upper-class *Internet and Computer Crimes* seminar. He has spoken throughout the United States as well as in Europe, Asia and the Middle East on white collar crime and cybercrime and has lectured on the subject of cybercrime at Harvard Law School.

Mr. DeMarco is a *Martindale-Hubbell* AV-rated lawyer for Computers and Software, Litigation and Internet Law, and is also listed in *Chambers USA: America's Leading Lawyers for Business* guide as a leading lawyer nationwide in Privacy and Data Security. He has also been named as a "SuperLawyer" for his expertise and work in the area of Intellectual Property Litigation.

**William H. Efron**

**Director, Northeast Region**

**Federal Trade Commission**

**William H. Efron is the Director of the Federal Trade Commission's Northeast Regional Office. On behalf of the FTC's Bureau of Competition, he oversees merger and conduct investigations and litigations. On behalf of the FTC's Bureau of Consumer Protection, he oversees investigations and litigations involving unfair, deceptive and fraudulent practices. Prior to joining the FTC, Mr. Efron was an associate at Simpson Thacher & Bartlett LLP. He received his J.D. from the University of Virginia School of Law and his B.A. from the University of Pennsylvania.**



**Esra Hudson's** practice focuses on all aspects of employment law and related litigation. She represents companies in state and federal court in claims of discrimination, harassment, wrongful discharge and related tort claims, breach of contract, trade secrets, and unfair competition, and all other employment-related matters. Ms. Hudson also defends companies against employment-based class actions. She regularly represents employers in proceedings before state and federal agencies, including the California Department of Fair Employment and Housing, the California Division of Labor Standards Enforcement and the federal Equal Employment Opportunity Commission. Ms. Hudson's litigation practice also includes extensive experience in alternative dispute resolution, including arbitration and private mediation.

In addition to a litigation practice, Ms. Hudson advises companies on a variety of employment and personnel management issues. She also regularly develops employment manuals and policies, as well as executive employment and severance agreements. Ms. Hudson provides a wide array of management training on a variety of employment-related subjects, including sexual harassment and discrimination prevention.

Ms. Hudson provides services for companies in a variety of industries, including entertainment, financial services, healthcare, transportation, insurance, manufacturing, the service industry and nonprofits.

#### **Education**

University of California Los Angeles School of Law, J.D., 1999.

Member and Symposium Editor, UCLA Law Review.

University of Wisconsin-Madison, B.A., with distinction, 1991

## **Keith Larney**

### **Position/Title:**

VP and Managing Assistant General Counsel

### **Firm or Place of Business:** CA Technologies

**Address:** 3965 Freedom Circle, Santa Clara, CA

**E-Mail:** Keith.Larney@ca.com

### **Primary Areas of Practice:**

Technology and Outsourcing Transactions, M&A, Corporate,  
SEC Reporting, General Practice

### **Law School/**

### **Graduate School:**

Boston College Law School, JD  
Harvard University, AB cum laude

### **Work History:**

#### **CA Technologies**

Head of North American Field Legal

Head of Global Partner Legal

Divisional General Counsel for Nimsoft, a CA subsidiary

AGC in M&A/Corporate and US West Field Legal

#### **i2 Technologies**

AGC for Technology Transactions, SEC reporting, M&A,  
Corporate and Marketing

#### **Law Firm Practice**

Corporate Associate, Jenkins & Gilchrist

Corporate Associate, Edwards & Angell



**JOSEPH J. LAZZAROTTI** is a Shareholder in the Morristown, New Jersey office of Jackson Lewis P.C. He founded and currently helps to lead 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**, which is part of the Firm's **Employee Benefits Counseling and Litigation Practice Group**.

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.

As part of Joe's work in the area of privacy, e-communication and data security, 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 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, business associates 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 businesses avoid breaches of personal and company data and achieve compliance. He has also represents 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 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*, *The National Law Journal*, *Financial Times*, *Business Insurance Magazine*, *Politico*, *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.

**Michele C. Lee**

**Michele C. Lee** is the Associate Legal Director of Litigation and Competition at Twitter Inc. In this capacity, she focuses on managing U.S. litigation for the company, including matters involving privacy, IP, unfair competition, and the First Amendment. She also counsels the company on competition matters. Before joining Twitter, Ms. Lee managed complex antitrust and patent litigation at Visa Inc., where she also advised internal business leaders about how competition laws could affect business strategy. Prior to joining Visa, Ms. Lee served as a Trial Attorney for the United States Department of Justice, where she litigated cases involving civil fraud committed against the U.S. government.

## **Scott Maples**

Scott is the former Vice President, General Counsel and Corporate Secretary of Ruckus Wireless, an innovative provider of Wi-Fi related equipment, software and services. At Ruckus, Scott built the legal department from the ground up, led Ruckus's IPO, and then managed all aspects of Ruckus's legal affairs as it scaled globally prior to its recent sale to Brocade Communications.

Prior to joining Ruckus, Scott was an AGC at Microsoft's Silicon Valley Campus where he lead teams supporting a number of incubating and growth technology businesses serving the internet, communications, consumer electronics and entertainment industries. Previously, Scott was VP, Business and Legal Affairs, for Virgin Interactive Entertainment, a videogame company within the Viacom family of companies. Scott began his legal career as a corporate and intellectual property associate at Stradling, Yocca, Carlson and Rauth, and was once an engineer for Hughes Aircraft Company where he developed software and managed a number of classified computer operations at Hughes' headquarters in Culver City, California and in Hahn, Germany.

Scott received a bachelor's degree in Computer Science, with Highest Honors, from UC Santa Barbara where he was a Regents Scholar and member of the Letters and Science Honors Council. Scott received his J.D. from Boalt Hall School of Law at the University of California, Berkeley where he was Managing Editor of what is now the Berkeley Technology Law Journal and was Editor-in-Chief of the Boalt Hall Cross-Examiner.

Scott is also the president of the Board of Directors of the Law Foundation of Silicon Valley.

**Christin McMeley**

**Christin McMeley**, CIPP/US, is the Chair of Davis Wright Tremaine's Privacy and Security practice. Christin advises companies in various industries in privacy compliance, information governance, data security, public policy, and regulatory matters. She advocates on behalf of clients before governmental agencies, legislative members and staff, represents telecom, cable, and wireless providers in regulatory proceedings before the FCC and counsels clients on regulatory policy and compliance. As a former Vice President, Chief Privacy Officer, and Deputy General Counsel to Charter Communications, Christin successfully implemented the company's first privacy and data security program. She and her team keep clients up to date on important privacy and security-related developments at [www.privsecblog.com](http://www.privsecblog.com).



### **Tyler G. Newby**

Partner

Litigation Group,  
White Collar / Regulatory Group

---

Phone: 415.875.2495

E-mail: [tnewby@fenwick.com](mailto:tnewby@fenwick.com)

---

#### **Emphasis:**

Privacy and Information Security

Regulatory and Internal  
Investigations

Copyright Litigation

Trademark Litigation

Trade Secret Litigation

**Tyler Newby** focuses his practice on privacy and data security litigation, counseling and investigations, as well as intellectual property and commercial disputes affecting high technology and consumer-facing Internet companies. Tyler has an active practice in defending companies in consumer class actions, state attorney general investigations and federal regulatory agency investigations arising out of privacy and data security incidents. In addition to his litigation practice, Tyler regularly advises consumer-facing Internet companies large and small on reducing their litigation risk on privacy, data security and secondary liability issues. Tyler frequently counsels game and social media companies on compliance with the Children's Online Privacy Protection Act ("COPPA").

In 2014, Tyler was named among the top privacy attorneys in the United States under the age of 40 by Law360. He currently serves as a Chair of the American Bar Association Litigation Section's Privacy & Data Security Committee, and was recently appointed to the ABA's Cybersecurity Legal Task Force.

Prior to rejoining Fenwick & West in 2011, Tyler was a Trial Attorney with the U.S. Department of Justice's Computer Crime and Intellectual Property Section. As a federal prosecutor, Tyler investigated and prosecuted intellectual property and cybercrimes nationwide, and advised federal law enforcement on compliance with the Fourth Amendment, the Electronic Communications Privacy Act, and other statutes pertaining to electronic surveillance and the search and seizure of electronic information.

While at the Department of Justice, Tyler also served as a Special Assistant United States Attorney in the Cyber Unit of the United States Attorney's Office for the Eastern District of Virginia in Alexandria, Virginia. As a Special Assistant, Tyler prosecuted fraud, intellectual property and computer intrusion offenses.

Tyler is an experienced trial lawyer. His courtroom experience has included serving as lead trial counsel on complex intellectual property and fraud matters, including the first criminal jury trial concerning the use of the BitTorrent protocol to facilitate criminal copyright infringement. Tyler also has extensive experience in handling *ex parte* and preliminary injunction procedures in both California and federal trade secret, copyright and trademark matters.

---

**FENWICK & WEST LLP**

### **Recent Privacy, Data Security and e-Commerce Litigation Representations**

- Obtained dismissal of putative class action brought against Internet security software developer alleging the software had been compromised from a prior cyberattack;
- Obtained dismissal of privacy and trespass to chattels claims against popular mobile radio streaming application.
- Representation of mobile application developers in putative consumer class action privacy and unfair competition cases;
- Obtained dismissal of complaint alleging business misrepresented the privacy practices of a competitor;
- Obtained dismissal of consumer class action claim brought against business alleging violation of California's anti-spam law;
- Representation of consumer software company in state and federal putative consumer class actions arising out of alleged security vulnerability;
- Obtained rare dismissal at the pleading stage of putative class action brought against mobile application developer alleging violation of the Telephone Consumer Protection Act.

### **Recent Privacy and E-Commerce Regulatory Representations**

- Represented major mobile advertising network in FTC investigation and enforcement action concerning inferring location data from Wi-Fi access points and compliance with COPPA;
- Advise numerous consumer-facing Internet companies on development of law enforcement compliance programs and in responding to law enforcement and regulatory agency requests for consumer data;
- Counseling to advertising networks on data collection and use practices;
- Representation of mobile device application developers in California Attorney General, U.S. DOJ, and FTC privacy investigations;



- Representation of companies in investigations of network security breaches;
- Representation of online travel site in DOT investigation regarding fare listings.

#### **Recent Intellectual Property Litigation Representations**

- Representation of major B2B Internet company in direct and secondary liability trademark infringement litigation;
- Representation of major video game publisher in copyright and computer fraud litigation concerning theft and distribution of pre-release version of game;
- Representation of computer device and component manufacturer in trademark infringement litigation over use of its house brand;
- Representation of mobile game publisher in trade secret litigation over hiring of software engineers.

#### **Recent Securities Regulatory and White Collar Representations**

- Representation of Fortune 100 company in internal investigation and related SEC and DOJ investigations into allegations of bribery and kick-back allegations;
- Representation of former public company officer in SEC Sarbanes-Oxley investigation and criminal prosecution;
- Internal investigation on behalf of audit committee into allegations of accounting and procurement improprieties;
- Representation of individuals in DOJ and SEC fraud and insider trading investigations and litigation;

Tyler received his J.D. degree from Stanford Law School in 1999 where he was a member, Notes Editor and Associate Editor for the *Stanford Law Review*. He graduated *summa cum laude* and Phi Beta Kappa, with an A.B. degree in history from Dartmouth College in 1996.

Tyler is a member of the State Bar of California and is admitted to practice before all federal district courts in California, the United States Courts of Appeals for the Federal Circuit and the United States Supreme Court.

---

**FENWICK & WEST LLP**

Tristan Ostrowski manages the Core Platforms legal team at Google, covering Android and Chrome OS. Tristan is also Senior Product Counsel for Android, and reviews launches and works with business and product teams on legal and regulatory issues related to the Android platform, mobile apps, and location services. He served as lead counsel on the past six major launches of the Android platform, and on the launches of Google Now, Google Play, and other Google mobile apps and services. In his roles, Tristan commonly deals with IP, privacy, security, competition, and consumer-protection issues. Prior to Google, Tristan was an attorney at Cleary Gottlieb, where his practice focused on IP and privacy issues for technology clients.

**Alison Pepper**

Former Assistant General Counsel and Senior Director of Public Policy  
Interactive Advertising Bureau

Alison Pepper is the Assistant General Counsel and Senior Director of Public Policy for the Interactive Advertising Bureau, based out of their San Francisco office. There she is responsible for a wide spectrum of in-house counsel work, including: contract drafting, contract review, contract negotiation, managing outside counsel, international trademark licensing, data privacy, IP licensing issues, HR issues, media, marketing, etc. . Before joining the Interactive Advertising Bureau, she worked as a Legislative Analyst for Experian, where she covered issues ranging from data security to identity theft. She has extensive experience working in state government, including the Georgia Senate and the Georgia Secretary of State's Office. She holds a B.A. from the University of Georgia and a J.D. from Georgia State University.

**Lucian T. Pera** is a partner with the Memphis, Tennessee, office of Adams and Reese LLP. His practice includes civil trial work, including commercial litigation and media law, and he counsels and represents lawyers, law firms, and others on questions of legal ethics and the professional responsibility of lawyers. A Memphis native, he is an honors graduate of Princeton University and Vanderbilt University School of Law. He served for five years on the ABA “Ethics 2000” Commission, which rewrote the ABA Model Rules of Professional Conduct. From 1995 through 2009, he led the Tennessee Bar Association Standing Committee on Ethics and Professional Responsibility. Under his leadership, the committee developed and successfully proposed to the Tennessee Supreme Court new legal ethics rules for Tennessee based on the ABA Model Rules of Professional Conduct. He has chaired the editorial board of the *ABA/BNA Lawyers’ Manual on Professional Conduct*, has served as president of the Association of Professional Responsibility Lawyers, and serves as a member of the Advisory Board for the Miller-Becker Institute for Professional Responsibility of the University of Akron. He is also the immediate past Treasurer of the American Bar Association, a former member of its Board of Governors and Executive Committee, and has served in the House of Delegates since 1990. He also serves as Vice President of the Tennessee Bar Association and will be its President in 2017.

Michelle Perez

Michelle Perez is Assistant General Counsel Privacy for the Interpublic Group of Companies (“IPG”), a global network of advertising and marketing communications agencies, where she is responsible for data privacy globally. Her duties include the development, implementation and management of data privacy policies, initiatives, strategies and programs.

Prior to joining IPG, Ms. Perez was Senior Privacy Counsel for Philips Electronics North America Corporation, a multi-national health and well-being company. In this role, she advised Philips’ businesses and functional organizations on data protection and privacy issues, managed data security incidents, and contributed to corporate efforts aimed at addressing emerging privacy and data protection requirements.

Ms. Perez is a Certified Information Privacy Professional, and a member of the 4As Privacy Committee.

Ms. Perez is a former Assistant United States Attorney for the Eastern District of New York. She received her J.D. from Fordham School of Law and her B.A. from Georgetown University.

**Noga Rosenthal**  
**Chief Privacy Officer, Epsilon**

Noga Rosenthal brings extensive experience in online advertising, legal issues and emerging technologies to Epsilon. In her role as Chief Privacy Officer, Noga oversees all privacy-related activities for Epsilon and its Conversant business, including global development, implementation, maintenance of and adherence to the organization's policies and procedures covering the privacy of, and access to, online and offline consumer data. Her responsibilities include ensuring compliance with various self-regulatory regimes as well as domestic state and federal laws and regulations and those of foreign jurisdictions.

Noga guides and advocates on behalf of Epsilon's internal teams, partners and clients to support industry self-regulation, responsible privacy practices, as well as consumer awareness, transparency and choice. Additionally, she monitors and helps guide the company's global public policy efforts.

Prior to Epsilon, Noga served as General Counsel and Vice President for Compliance and Policy for the Network Advertising Initiative (NAI), leading their compliance program and ensuring that member companies delivered on the promise of self-regulation for interest-based advertising. Previously, she held the role of Senior Vice President and General Counsel of WPP plc companies Xaxis and Media Innovation Group, LLC.

Noga sits on the Board of Directors of the NAI and sits on the Advisory Board of the Digital Advertising Alliance, the Legal Affairs Council and the Public Policy Council of the Interactive Advertising Bureau and has served in the past on the International Association of Privacy Professionals Education Advisory Board.

Noga holds a Bachelor of Arts degree in English and Political Science from the Rutgers College and a J.D. from Fordham Law School.

## **Keith Yandell**

**Keith Yandell** currently serves as both the General Counsel and Head of People at DoorDash, Inc. Before becoming DoorDash's first General Counsel, Mr. Yandell worked as Director of Litigation at Uber Technologies, Inc. While at Uber, Mr. Yandell managed numerous high profile matters including the company's primary independent contractor misclassification class action, a class action stemming from Uber's self-reported data breach, and an Unfair Competition Law case prosecuted by the Los Angeles and San Francisco District Attorneys. In advising on these and other matters, Mr. Yandell worked closely with Uber's executive team, including its General Counsel, Head of Communications, and CEO. Prior to joining Uber, Mr. Yandell was an Equity Partner at Allen Matkins LLP, where his practice focused on complex class actions, particularly in the financial services space.

Mr. Yandell obtained his law degree from the UCLA School of Law, and his undergraduate degree from the University of California at Davis.

## JOHN C. YATES

### **Partner / Chair – Corporate Technology Group Morris, Manning & Martin, LLP**

404.504.5444 | [jyates@mmmlaw.com](mailto:jyates@mmmlaw.com) | [linkedin.com/in/johnnyates](https://www.linkedin.com/in/johnnyates) | [@jcyates](https://twitter.com/jcyates)



Mr. Yates is chair of the Corporate Technology Group of Morris, Manning & Martin in Atlanta. He is internationally recognized in the technology law and corporate finance fields. His firm represents technology companies in all stages of growth and is a leader in VC and private equity deals, IPOs and M&A transactions. Mr. Yates is co-founder of the Technology Association of Georgia, Southeastern Software Association, and Southeast Medical Device Association. He has authored hundreds of articles and was cited by the U.S. Supreme Court in *Kodak vs. Image Technical Services*.

He received his B.A. and J.D. from Duke University and serves on the Board of Visitors at the Duke School of Law and Board of Trustees of Furman University. Mr. Yates was chair of the 2013 NCAA Final Four Basketball Tournament in Atlanta in April 2013.



**Bonnie L. Yeomans**

**Position/Title:** Assistant General Counsel and Chief Privacy Officer

**Firm or Place of Business:** CA Technologies

**Address:** 1 CA Plaza, Islandia, NY

**Phone:** 631-342-2678

**Fax:** 631-342-4866

**E-Mail:** bonnie.yeomans@ca.com

**Primary Areas of Practice:** Data Privacy

**Law School/**

**Graduate School:** Benjamin N. Cardozo School of Law

**Work History:** Member of Worldwide Law Department within CA Technologies since 1990, serving in various legal capacities, including software licensing, advertising, real estate, regulatory compliance, and ethics and compliance. Chief Privacy Officer since 2004.

**Professional Memberships:** IAPP (International Association of Privacy Professionals) membership, with CIPP certification.

1

Emerging, Disruptive and Sharing  
Technologies: What Is the Sharing Economy  
and Where Is It Going? (December 10, 2016)

John C. Yates

*Morris, Manning & Martin LLP*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



## **WHAT IS THE SHARING ECONOMY?**

1. **Definition.** Over time, the sharing economy has developed many different names and terms (collaborative consumption, collaborative economy, on-demand services, and peer economy), that most users treat as synonyms for the sharing economy, thereby grouping them all under the same umbrella. While many of them have overlapping definitions, each term still differs slightly.<sup>1</sup> For the purposes of this article, we will use the term “Sharing Economy” to discuss this disruptive economic paradigm as a collective. However, it is important to identify the differences between the companies of the Sharing Economy, so the following umbrella vocabularies are defined individually.
  - a. *Sharing Economy* - the sharing economy is a system or business model that focuses on sharing underutilized assets, either for free or for some form of compensation, between either businesses or individuals.<sup>2</sup> The transaction is usually set up and paid for through an online forum.<sup>3</sup> For example, Fon allows members to share one another’s Wi-Fi hotspot.
  - b. *Collaborative Consumption*- those events in which people utilize goods or services by engaging in joint activities with one or more others.<sup>4</sup> It is a system that focuses on providing access to goods and services over ownership through trading, sharing, or renting.<sup>5</sup> Chegg is a company that allows users to rent books, and Cohealo is a company that allows hospitals to share equipment when it is not being used.
  - c. *Collaborative Economy* - a system that matches ‘needs’ and ‘haves’ in order to allow people to make use of underutilized assets in a way that bypasses the traditional market for that good or service.<sup>6</sup> Uber matches those that need a ride to a certain destination with those that have a car and are willing to drive for a fee through smartphone technology.

---

1. Rachel Botsman, *The Sharing Economy: Dictionary of Commonly Used Terms*, A Medium Corporation (October 19, 2015), <https://medium.com/@rachelbotsman/the-sharing-economy-dictionary-of-commonly-used-terms-d1a696691d12#a528xypnm>.
2. *Id.*
3. Yates, *supra* at note 10.
4. BUCZYNSKI, *supra* note 1, at 4-5.
5. Botsman, *supra* note 24.
6. *Id.*

- d. *Gig Economy* - the gig economy breaks up a traditional paid company position into individual “gigs” that are distributed to independent workers to be paid per transaction or service.<sup>7</sup> For example, Taskrabbit is a company that assigns each task to an individual, whether it is going to the grocery store or cleaning a house, and the worker is paid for each separate task.
- e. *On-Demand Economy* - the on-demand economy satisfies consumers’ immediate needs by instantly connecting them with a provider to deliver the goods or services desired at that time.<sup>8</sup> Uber can also operate under the on-demand economy umbrella because the company instantly provides a driver to escort the user from point A to point B.
- f. *Peer Economy* - the peer economy operates solely between private individuals to exchange goods or services when needed.<sup>9</sup> Etsy is an example of peer-to-peer transactions whereby one individual provides a good that the other individual may purchase.

This article focuses on certain regulations and challenges that disruptive, Sharing Economy companies may face in the United States, although there are certainly challenges that these companies confront abroad. Additionally, any references to legal challenges faced by certain Sharing Economy companies merely serve as examples and by no means reflect upon the legality of that company’s activities.

1. **Many Players.** While you have probably heard of Uber, Lyft, and Airbnb, you may not have heard of WeWork (workspace sharing), Fon (home Wi-Fi networks), Feastly (food sharing), PostMates (personal couriers), TaskRabbit (personal services), Bellhops (moving services), Shipt (grocery delivery services), Forge (3D printing) or Rubicon Global (waste collection).
2. **Examples of Assets.**
  - a. Hospitality (Spaces): Hospitality or space is a popular area for the sharing economy. With vacation homes, spare bedrooms, and vacant apartments, it lends itself well to the sharing system. Airbnb is the most well-known of the hospitality startups, allowing individuals to rent out spaces for their travels at a

---

7. *Id.*

8. *Id.*

9. *Id.*

cheaper rate than a standard, traditional hotel. In 2015, Airbnb was valued at \$13 billion and operates in 20 different cities worldwide with over 50,000 renters per night.<sup>10</sup> While Airbnb continues to control the personal side of the hospitality market, there are also workspace companies that rent out extra offices or space to other workers such as ShareDesk and WeWork.<sup>11</sup> Airbnb and other hospitality startups encourage consumers to travel and get out, and therefore, the future for the sharing economy and the hospitality industry will likely continue to grow.

- b. Skilled and unskilled time: The most well-known of the skilled and unskilled time services startups are TaskRabbit, Zaarly, and DogVacay. Both TaskRabbit and Zaarly allow users to describe the task they want accomplished and then pair a provider to complete that task.<sup>12</sup> Tasks include a range of activities from basic home improvement to grocery shopping and other errands to cleaning. DogVacay allows users to find sitters for their pets whether it is to simply come by once during the day or board the animal overnight. The site allows the option of keeping the animal at home or with the sitter. Other companies in this space include: EatWith, Feastly (cooking); Rubicon (waste collection); and Bellhops (moving services).
- c. Financial Services: The money/financial industry looks at lending, crowdfunding, and cryptocurrencies.<sup>13</sup> Lenders include those startups where individuals can lend or receive money without having to go through a traditional financial institution. These include businesses like LendingClub and Zopa. Crowdfunding is probably the most popular of these money services. Sites like GoFundMe allow large groups of people to donate to a cause, and users can fundraise support. Cryptocurrencies, such as bitcoin, create their own type of currency and allow users to make exchanges.
- d. Temporary use of goods: The goods industry can also be divided into three separate categories: maker movement, loaner products, and pre-owned goods.<sup>14</sup> Etsy is the leader of the

---

10. *The Sharing Economy: Consumer Intelligence Series*, *supra* at note 18, at 23.

11. OWYANG, *supra* note 43.

12. Schor, *supra* note 9.

13. OWYANG, *supra* note 43.

14. *Id.*

maker movement. It allows crafters and creators to post the products they make on the site where users can then directly order them. Loaner products, like Rent The Runway, loan out their products temporarily to users who then return them once they are finished. Rent The Runway is a successful company that allows women to rent designer label dresses for formal occasions for a fraction of the price it would be to buy the name brand item. eBay and Craigslist remain the leaders of the pre-owned goods business, allowing buyers and sellers to exchange goods. Other companies in this sector include LeftoverSwap (extra portions of food); Neighborgoods (extra goods); Amazon Family Library, Netflix, Spotify, and SoundCloud (media).

- e. Food: The Sharing Economy food industry can be divided into three subparts: food delivery, shared food, and shared food prep.<sup>15</sup> Food delivery itself is not a new concept. Pizza has been delivered for quite some time now, but companies like Uber Eats bring food delivery into the sharing economy. Uber Eats posts a menu each week of the various local restaurants and specific menu items available for order and delivery. The Uber drivers then pick up the food and deliver them to the users that requested it. Shared food startups, such as Feastly, allow users to find a provider hosting a home cooked meal in their city.<sup>16</sup> Chefs take advantage of food sharing as well in that they enjoy hosting meals and experimenting with foods while socializing with new and different people in their own homes. Food share prep companies, like Munchery<sup>17</sup>, make meals and deliver them directly to the user's door, or if the user does not live within a reasonable distance, the company will deliver the ingredients needed to cook the meal.
- f. Combination any of these (e.g., while Getaround connects buyers with the use of a car, Uber connects buyers with the use of the car plus use of a driver's time).

---

15. OWYANG, *supra* note 43.

16. *Id.*

17. *Id.*

## **ORIGIN OF THE SHARING ECONOMY**

3. **Not New.** Despite the huge amount of press that the Sharing Economy has received lately, it is not an entirely new concept.
  - a. For example, throughout history individuals have participated in the Sharing Economy through:
  - b. **Event Parking.** Paying for parking at a sporting event or concert by “renting” an unutilized parking space at a home or business that is empty or closed at the time of the event.
  - c. **Boarding Houses.** Mentioned in films ranging from “It’s a Wonderful Life” to “Forest Gump”, boarding houses are historical examples of the Sharing Economy – unused rooms in a private home being used by travelers seeking temporary lodging.
  - d. **Carpooling.** Coworkers and friends have used carpooling to reduce the cost of commuting by sharing fuel costs and cars for decades, particularly in the post-war years.
4. In 1978, Marcus Felson and Joe Spaeth created the term “collaborative consumption” when they published the article “Community Structure and Collaborative Consumption: A Routine Activity Approach” in the *American Behavioral Scientist*. The article described the new concept of car sharing, an evolution from the previous carpooling idea during World War II.<sup>18</sup>
  - a. “Collaborative consumption” was defined as “those events in which one or more persons consume economic goods or services in the process of engaging in joint activities with one or more others.”<sup>19</sup>
  - b. This publication was the first real glimpse into what makes up the modern sharing economy today.
  - c. From the idea of collaborative consumption, or peers working together for a mutual benefit, eBay and Craigslist were born around 1995.<sup>20</sup>

---

18. **BUCZYNSKI**, *supra* note 1, at 17.

19. *Id.*

20. Juliet Schor, *Debating the Sharing Economy*, **GREAT TRANSITION INITIATIVE** (October 2014), <http://www.greattransition.org/publication/debating-the-sharing-economy>.



5. **What Is New Is The Scope.** A 2015 PricewaterhouseCoopers study (the “PwC Study” found at: <http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/pwc-cis-sharing-economy.pdf>) estimated that the international Sharing Economy reached \$15 billion in 2015 and is expected to reach \$335 billion by 2025. Three major forces came together at the right time to provide exponential growth in the Sharing Economy:
- a. **Economics.** The Great Recession of 2008 forced many individuals to reconsider the necessity of possessions and consider alternative sources of income.
    - i. More individuals were forced to accept the idea of renting out a room in their home to a stranger or driving for a ride-sharing service in their spare time. Similarly, individuals had to look to alternative means to obtain goods and services as they could no longer afford the large expense of purchasing a good that they may use infrequently.
  - b. **Technology.** Second, the growth of the Internet and widespread use of social media and mobile devices decreased transaction costs and increased transparency and accessibility for these Sharing Economy companies.
    - i. Sellers and service providers can enter the market more easily through lower startup expenses, low-cost advertising and app development.
    - ii. Technology and social media allows new entrants to reach a broader audience more easily.
    - iii. Buyers can use GPS-enabled smartphones to find the nearest available room, car, or home cooked meal.
    - iv. Both parties can use social media and background check services to ensure the trustworthiness of the other party and rate and provide feedback on their experiences.
    - v. Provides low cost options for payment processing, such as credit cards and mobile payments.
  - c. **Culture.** Third, changes in our values have aligned with the strengths of the Sharing Economy.
    - i. Younger people often do not place value in the ownership of goods and instead value access to the functionality that the goods provide. This is similar to the shift away from

directly installing software on computers to providing access to the software remotely via a software-as-a-service model.

- ii. Many people of all ages are more environmentally concerned. For example, the Center for a New American Dream reported that 91% of Americans believe that the way we live produces too much waste. By using idle assets rather than buying new assets, the Sharing Economy can reduce society's overall demand for resources. A University of California - Berkeley Transportation Sustainability Research Center study ([http://www.uctc.net/access/38/access38\\_carsharing\\_ownership.pdf](http://www.uctc.net/access/38/access38_carsharing_ownership.pdf)) suggests that for every car available to share, between 9 and 13 cars are eliminated from private ownership. Further, ZipCar estimates that every Zipcar eliminates at least 20 cars from private ownership.

## **WHERE IS THE SHARING ECONOMY GOING?**

6. **Future Growth.** Although the term has only been used since the mid-2000s, the Sharing Economy has already taken off in the past half-decade, and will only continue to grow.
  - a. It has been a busy few years for the Sharing Economy. With Airbnb's \$10 billion valuation surpassing Hyatt Hotels and Uber's \$18.2 billion valuation surpassing rental car giants Hertz and Avis, 2014 marked the year that the Sharing Economy officially graduated from couch surfing startups to major businesses.<sup>21</sup>
  - b. In 2015, however, the Sharing Economy hit serious legal and political snags. San Francisco's Proposition F (aka the "Airbnb Initiative") was designed to put serious restrictions on private, short-term rentals and the company waged a tone-deaf public relations battle with the city. Uber is battling a class action lawsuit in California, regulation push back in cities from

---

21. **Brian Hughes**, *Collaborative Consumption: What's Next for the Sharing Economy in 2016?* (December 2016), <http://www.greattransition.org/publication/debating-the-sharing-economy>.

London to New Delhi, and a public relations nightmare as some Uber drivers have been convicted of raping their passengers.<sup>22</sup>

- c. **Analogous to Online Shopping.** The Online Economy started out small and tentative just like the Sharing Economy. But then it grew because parties learned to trust each other, concerns about credit card theft were largely resolved, and novel legal issues were addressed.
  - d. **Societal Shifts.** Projected demographic and economic shifts may increase the popularity of the Sharing Economy.
    - i. With the uncertainty of social security benefits and rising cost of college tuition, there will be a rapid growth in retirees, parents and students seeking part-time income, a strong characteristic of the Sharing Economy.
    - ii. Since the Great Recession, there has been a continued shift in the value of ownership as more individuals rethink the necessity of possessions and the societal status that these possessions bring.
  - e. **Chicken or the Egg?** With greater prevalence in our society, more individuals are accepting of the Sharing Economy. For example, in the PwC Study, among US adults already familiar with the Sharing Economy, 72% said that they could see themselves continuing to be a consumer in the Sharing Economy in the next two years.
  - f. **Greater Competition.** As more companies enter into the same industry in the Sharing Economy (e.g., Uber, Lyft, Sidecar), fees are kept low to encourage consumer participation. For example, Uber promotes lower fees by 20% during the winter holiday season. These lower fees will encourage more consumer participation in the Sharing Economy.
7. **Business Benefits of Sharing.** More businesses will continue to seek the business benefits of operating in the Sharing Economy, such as:
- a. **Being Asset-Light.** Sharing Economy companies do not have to own large fleets of cars, consumer goods, or even build hotels to be able to provide these goods and services, thereby reducing

---

22. *Id.*

inventory and fixed asset costs. Further, these companies do not have to pay to maintain and update goods that they offer.

- b. **Lower Labor Costs.** While Sharing Economy companies maintain full-time staff, these companies generally have fewer employees and therefore ultimately pay less in salaries and benefits and can rent smaller office spaces.

## **CASE STUDY OF THE SHARING ECONOMY – RUBICON GLOBAL**

- 8. **Waste and Recycling Sharing.** Rubicon Global connects small, independent waste and recycling haulers with consumers and businesses in an effort to deliver sustainable waste management services and cost reduction. Rubicon has 60,000 locations where its network of haulers can pick up garbage or recycling.
  - a. **Innovative Technology.** Rubicon uses big data and a cloud-based software platform to enable efficiencies in waste and recycling pickups. Customers use Rubicon's platform to schedule a pickup when the customers' dumpsters are actually full, rather than regularly scheduled pickups that might not be needed. Cameras can also monitor dumpster levels and sensors can indicate and confirm when pickups actually happen.
  - b. **Sharing Economy.** Allowing customers to customize their waste pickups gives smaller, independent haulers greater access to more customers and an opportunity to become part of the Sharing Economy. This also reduces the cost of pickups for customers by eliminating unnecessary pickups and requiring haulers to bid for jobs.
- 9. **Disrupting an Outdated Industry.** The waste industry is dominated by large companies such as Waste Management and Republic Services and, similar to the taxi industry and Uber, has seen very little technological innovation.
  - a. **Rubicon's Growth.** Rubicon has raised \$30 million in funding in January 2015 and \$50 million in September 2015; valued at \$500 million; doubled in size every year for the past three years and has become the largest third party provider of waste and recycling in North America.
- 10. **Beyond the Rubicon Business Model.** Many companies in the Sharing Economy focus on societal goals in addition to profits.

- a. **Sustainability.** Rubicon's model reduces local emissions and greenhouse gases from fewer truck pickups; diverts waste streams from landfills and incinerators to appropriate recycling facilities with the goal to create zero waste for 100% of Rubicon's customers by 2022.
- b. **Rubicon X Research & Development.** Rubicon runs a research and development lab where the company tests new recycling technology that will help make waste obsolete.

## **CURRENT LEGAL ISSUES FOR THE SHARING ECONOMY**

11. **Start the Business, then Address Regulation Approach.** Sharing Economy companies tend to approach regulatory challenges differently than traditional companies.
  - a. **Traditional Approach.** A traditional company is more likely to try to address or change the regulatory landscape before entering into business. This due to the high initial investment required to start a business and the fear that the company will later be regulated out of profitability.
  - b. **Sharing Economy Approach.** However, because Sharing Economy companies do not face the same level of initial investment, they are more likely to start doing business without first resolving potential regulatory hurdles. They then negotiate with regulators while continuing to do business.
  - c. **Public and Political Support.** This allows the Sharing Economy company to develop public acceptance and leverage their position. For example, banning Uber or Airbnb after consumers have experienced them will make some consumers unhappy, which may worry elected officials.
  - d. **Increased Consumer Activism.** Because Sharing Economy companies have access to their user's digital information they are very effective at persuading their users to digitally lobby elected officials. For example, in August 2015, Uber sent its customers in Boston an email encouraging them to reach out to their state legislators and voice opposition to a proposed bill that would impose new regulations on Uber and its drivers.
  - e. **Continuing to Gain Consumer Support against Legislators.** Additionally, these Sharing Economy companies can position themselves as the consumer's champion in opposition to

burdensome legislators. For example, Uber has gained support from consumers and privacy advocates in its public attempts to push back against legislation that requires disclosure of certain trip information.

12. **Challenges to Sharing Economy.** Challenges to Sharing Economy companies tend to fall into two broad categories:

- a. **Economic Justifications.** These arguments center on the value of limiting suppliers in an industry and typically come from incumbent businesses or interested parties. For example, the taxi medallion system in New York is justified as a way to protect the “retirement fund” of owners of those medallions. In some industries this is an example of Regulatory Capture, whereby regulators are more interested in protecting those regulated than the public.
- b. **Consumer Protection.** Many challengers question whether these Sharing Economy companies can provide the same level of safety as traditional businesses since they are often not held to the same legal and regulatory standards used to protect consumers. Sharing Economy companies typically respond in three ways; the sophistication and public acceptance of the Sharing Economy company typically influence its response.
  - i. Arguing that the regulation does not apply to them. For example, Uber claims that it is a matchmaking service between riders and drivers and not a provider of transportation services; therefore Uber argues that it is not subject to the laws applicable to taxi companies.
    1. Unfortunately, this argument does not always work. For example, Uber drivers in New York City are now subject to many taxi requirements, such as obtaining a TLC license, the Uber vehicle must have TLC plates and be affiliated with a base and have enough insurance to merit a FH-1 (for hire) card.
  - ii. Arguing that the regulations are out-of-date or anti-innovation. Many consumer protection regulations were enacted to address the Asymmetrical Information Problem, whereby a consumer does not have access to information about the seller or product until it is too late. However, Sharing Economy companies argue that they have solved the Asymmetrical Information Problem

through technology. For example, you cannot tell if a taxi is clean until after you get in and, therefore, regulations require regular inspections to ensure that taxis are properly maintained. However, Uber claims that such regulations don't make sense when applied to Uber's business model because passengers can see how other passengers have rated specific drivers prior to getting in the car. Drivers who have vehicle cleanliness issues will receive poor rating, passengers will not ride with them, and those drivers will be driven out by competition.

- iii. Complying with the spirit of the regulation but not admitting that the regulation applies to their company. For example, although it maintains that state and local regulations that require minimum amounts of insurance don't apply to the company, Uber maintains a national \$1M hybrid insurance policy that covers drivers while a passenger is in the car. This vastly exceeds amounts required by most state and local regulations applicable to taxis.

13. **Traditional Legal Issues.** Many legal issues that Sharing economy companies face arise out of traditional legal issues.

- a. **Misrepresentation.** For example, in December 2014, San Francisco and Los Angeles sued Uber under consumer protection laws, alleging that Uber misleads its riders on the rigor of its background checks and appropriate of fees. A similar civil suit in Connecticut was dismissed in August 2015, but the case filed by Los Angeles and San Francisco was settled in April 2016 for \$25 million. Under the terms of the settlement, Uber paid \$10 million to the cities of San Francisco and Los Angeles with the remaining \$15 million penalty being waived in two years if Uber complies with all of the settlement's terms which include provisions such as restrictions on where the company can operate and renaming its "safe ride" fee to a "booking" fee.
- b. **Neglect and Fraud.** Similar to claims of misrepresentation, these Sharing Economy companies may face lawsuits claiming neglect and fraud for failing to appropriately screen their service providers.
  - i. In July 2016, a woman from West Hollywood sued Uber in the Superior Court of California, accusing the company

of negligence after an Uber driver sexually assaulted her. The woman claimed that Uber markets the company as a safe transportation option, but fails to appropriately screen drivers.

- ii. In response to numerous instances of negligence of fraud claims, Uber hired Former Boston Police Commissioner Ed Davis as a safety consultant as the company prepared for a hearing to determine new regulations for ride-hailing services.
- c. **Data Protection.** While traditional companies must worry about data protection and privacy, even the smallest Sharing Economy companies also need to take steps to address data protection and privacy, as most Sharing Economy companies use GPS technologies, automatic credit card payment and a wealth of stored data to provide and improve their services.
  - i. As an example, the New York general manager accessed the Uber travel data of another journalist without her permission. Further, the company used a “God view” tool to track customer’s location at a launch party.
  - ii. Beyond legal compliance, how Sharing Economy companies manage access and control of data is essential to building customer trust and a business reputation.
- d. **Contractor/Employee.** The inventory of Sharing Economy companies is generally provided by a vast number of individuals, whom the Sharing Economy companies claim are independent contractors. There are different rules for determining who is an employee or a contractor depending on the applications – different federal laws, state laws, and regulations.
  - i. A class-action lawsuit against Uber in the U.S. District Court for the Northern District of California (O’Connor v. Uber Technologies, Inc. et al, C13-3826 EMC) over whether Uber drivers are independent contractors or employees, which affects payment of expenses, whether drivers may be fired at will, how many hours drivers work, entitlement to certain benefits, ability to form unions, etc. was recently settled, under which Uber would pay up to \$100 million and make significant changes in its policies.



- ii. However, in August 2016, the court declined to approve the settlement. The court's concern was largely with the settlement's reduction in the massive potential penalties that could be recovered (mostly for the State of California) under the Private Attorney General Act (PAGA).
  - iii. Because of this development, and a recent ruling in a related case, it is possible that the class in this case may be reduced to the few Uber drivers who opted out of arbitration (or who stopped working for Uber before the arbitration clause was first introduced in August 2013).
  - iv. In a related case regarding background checks, the Ninth Circuit Court of Appeals reversed the judge in the case on his ruling that Uber's arbitration clause is not enforceable.
  - v. There is a separate appeal pending in that case in which the argument is that Uber's arbitration clause is not enforceable for a different reason – because it violates the drivers' rights under the National Labor Relations Act to engage in concerted activity.
  - vi. The outcome of these cases could greatly affect the entire Sharing Economy, as other Sharing Economy companies, such as Lyft, Handy, TaskRabbit, Postmates and Door Dash, classify their workers as independent contractors.
14. **Miscellaneous Other Issues.** Depending on the specific sector and business model, there are a myriad of other unresolved potential issues for Sharing Economy companies.
- a. **Insurance and Liability.** Particularly for ride- and car-sharing services, but also for renters and homeowners providing room and house rentals, how will insurance be structured when other people are using the insured asset and which party (the Sharing Economy company or driver/homeowner) will be liable if a consumer is injured?
  - b. **Zoning Laws.** Are current zoning regulations and other rules governing short-term rentals applicable to these companies?
    - i. In New York, Gov. Andrew Cuomo signed into law in October 2016 new legislation that will only allow rentals of rooms where the host is also living there, and imposes fines up to \$7,500 on those who advertise rentals fewer than 30 days in multiunit buildings without the permanent

- resident's presence. Airbnb has responded by filing suit against New York arguing it is not responsible for what users post on their site.
- ii. Some renters have been served eviction notices and faced lawsuits from landlords for placing their homes on home-sharing services; neighborhood associations have also adopted rules to restrict short-term rentals.
- c. **Accessibility and Anti-Discrimination.** As Sharing Economy companies do not have direct control over service provider and consumer interactions, how do these companies monitor accessibility and ensure anti-discrimination policies are followed? What procedures must these companies implement for reporting discrimination?
- i. In August 2016, the New York Times ran an op-ed piece entitled, *Does Airbnb Enable Racism?* in which it cited a Harvard Business School study that showed requests from Airbnb guests with distinctively African-American names were 16 percent less likely to be accepted than those with white-sounding names. The article suggests that the home-sharing platforms may be in violation of several statutes including the Civil Right Act, the Fair Housing Act, and the prohibition against discrimination in contracting
  - ii. In September 2016, Airbnb announced a series of new policies to address the issue of discrimination on its website. Led by several prominent advisers, including former United States Attorney General Eric H. Holder, the policies were designed to quiet the questions over discrimination that have threatened to cloud growth of the company.
- d. **Trust and Safety Concerns.** While many Sharing Economy companies state that they provide routine background checks on their service providers, there is no guarantee that these companies are following through. As referenced, there have been numerous stories of ride-sharing drivers assaulting riders, for whom evidence of previous criminal convictions would have been discovered. Conversely, there is no guarantee that a consumer is trustworthy and will take care of property that it obtains from the Sharing Economy company or one of its users.

## **TAKE AWAYS**

15. The Sharing Economy is not new, but rapid technological and societal developments have caused it to grow extremely quickly and our traditional legal system is struggling to keep up with these non-traditional methods of doing business. The Sharing Economy's rapid success and continued societal shifts indicate that the Sharing Economy is here to stay.
16. So far, the legal issues facing the Sharing Economy are being handled in both the business and political arenas. However, as the losers and winners emerge from those discussions, we can expect more specific regulations and guidance to emerge.
17. Representatives of Sharing Economy companies need to worry about traditional problems as well as novel issues and should keep a close eye on the employee/contractor issue and anti-discrimination issue, as those issues could result in a major stumbling block for future growth of the Sharing Economy.

## NOTES

## NOTES

2

## The Virtual Workplace (December 9, 2016)

Joseph J. Lazzarotti

*Jackson Lewis P.C.*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



For most employers, 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. This is all happening over a national and international patchwork of laws, sometimes specific to certain industries, that is slow to develop and frequently in conflict.

In short, harnessing the power of the digital age while controlling workplace and related risks is a challenge, one that is not likely to get easier anytime soon. This article is intended to summarize those risks for employers, and help them to understand the kinds of steps they might want to take, and not take, to minimize those risks. We recognize that for most employers, employee privacy and data security considerations are changing rapidly, almost daily. So, we touch on several important developments and emerging issues for human resources professionals.

These materials will cover:

- BYOD Risks and Remote Access
- Using Social Media in the Hiring, Discipline and Termination Process
- Employee Monitoring
- California's Definition of "Reasonable Safeguards" for Protecting Personal Data
- Controlling Employee Data Security Risks

## **I. BYOD RISKS AND REMOTE ACCESS**

For a variety of reasons, including significant cost savings and employee relations, businesses have been considering or have already transitioned to a "bring your own device" ("BYOD") platform. In short, BYOD refers to arrangements where employees are permitted to connect their own personal devices to the employer's networks and systems to complete job tasks and access company and personal information from just about anywhere. Of course, many of the same concerns and risks that exists with BYOD are also present with other forms of remote access – e.g., working from home using a company or employee-owned laptop.



Many of the privacy and data security risks and issues covered above are enhanced when employees are permitted to use their mobile personal devices in this way. Moving in this direction has many benefits, but also creates a number of business and legal risks. Whether a business is “compliant” concerning BYOD will depend on a number of factors including industry, location, classes of data maintained on the device, governing regulatory agencies, professional/industry standards, contracts with business partners and other issues. BYOD also can result in some unintended consequences. These items are summarized below.

- **HIPAA and state data security requirements.** Even with new developments in device management software applications, the ability to manage and secure important company data and personal information is made more difficult with BYOD. The tightening of requirements to safeguard personal data under various federal and state laws (e.g., HIPAA, GLBA, and state mandates referred to above) and to quickly react to data breaches enhance this concern. Problems can arise in a variety of ways, such as the rogue employee who refuses to return the device, a challenge to whether a trade secret had been appropriately safeguarded, or a diligent employee who happens to inadvertently use an unsecure wireless network.
- **e-Discovery.** When involved in a litigation, having ready access to information required in the course of the discovery phase of the case can be made more complicated when some of that information may be stored on an employee’s personal device.
- **Wage and hour.** BYOD and personal communication devices can further blur the lines between personal and work time, raising the issue of whether time is compensable. Consider, for example, the employee on an employer-approved leave who spends hours each day responding to work-related emails. This is a challenge employers have to consider and address through carefully drafted and consistently enforced policies and procedures.
- **International data privacy requirements.** BYOD needs to be considered even more carefully when implemented on a global scale. Cross border transmissions of personal data and different employment standards from country to country can raise thorny issues for multinational companies.
- **Garden variety workplace law issues.** Workplace harassment, discrimination, and privacy risks are not avoided because suspect activities happen on an employee’s device, rather than the company’s

device. For example, an employee's sending harassing emails to other employees using his or her personal device still can raise discrimination and other issues for the company. Likewise, businesses that engage in monitoring employees' locations and communications may need to think more carefully about the nature, scope and notification requirements concerning that kind of monitoring activity when applied to the employee's personal device. An awkward employee relations issue (as well as an e-discovery risk) results when an employer utilizes the ability to "wipe" a device such as in the event of a security risk to the information on the device.

- **Labor.** A company considering BYOD for a group of employees represented by a bargaining group likely will need to bargain with the union on whether it can implement such a program.
- **Record retention and destruction requirements.** One of the concerns in a BYOD context is triggered when an employee changes his or her device. Tossing the device in the trash, even if in an environmentally friendly way, may not be consistent with federal or state data disposal requirements.
- **Reimbursement.** Although not a privacy and security issue *per se*, a recent decision in California may impact BYOD programs nationwide. In Cochran v. Schwan's Home Service, Inc.<sup>1</sup>, a California appellate court found that Section 2802 of the state's Labor Code requires employers to reimburse their employees when the employees must use their personal cell phones for work-related calls. The amount of reimbursement, the court declared, is a "reasonable percentage" of the personal cell phone bill.

## II. **USING SOCIAL MEDIA IN THE HIRING, DISCIPLINE AND TERMINATION PROCESS**

Employers are increasingly turning to social media for information about job applicants, yet these sources are replete with information, some of which is not accurate, that should not be considered in the hiring process. A Jobvite Social Recruiting Survey found, for example, that 92 percent of respondents plan to use social media for recruiting; the same survey found that LinkedIn, which may contain information that should not be

---

1. 228 Cal. App. 4th 1137 (2014).

considered when searching for or selecting candidates, is the most popular social networking site for recruiters.<sup>2</sup>

Generally speaking, so long as the employer does not violate state or federal discrimination laws, nothing currently prohibits an employment decision based on information an applicant places in the public domain. However, when using social media to vet job candidates, an employer may inadvertently become aware of certain information or characteristics of an applicant (including a current employee seeking a different position in the company) that can expose the employer to risk of a lawsuit if the employer makes a decision adverse to the individual based on that information or characteristic.

Here are some examples:

- **Federal and state discrimination laws.** Various federal and state laws prohibit employers from basing a hiring decision on an applicant's race, age, sexual orientation, marital status, disability and even genetic information, which are all protected under federal law.<sup>3</sup> In the case of genetic information, the law is relatively new and its proscriptions are in some respects somewhat counter-intuitive. Under the Genetic Information Nondiscrimination Act ("GINA"), "genetic information" includes, among other things, the manifestation of disease in a "family member," a term that is defined to include an applicant or employee's spouse, despite no genetic connection.<sup>4</sup> The general rule under GINA is that genetic information cannot be collected by an employer or used for an employment purpose, unless an exception applies. Thus, for example, purposefully searching for more information on Facebook about the health of an applicant's spouse (perhaps because of concerns of significant cost to the company's medical plan or increased need for the employee to take leaves of absence) is prohibited under GINA.

Some states also prohibit discrimination on account of sexual orientation, genetic information, disability status, political affiliation, receiving workers' compensation benefits, and lawful off-duty conduct. State laws prohibiting discrimination on the basis of lawful off-duty

---

2. Jobvite Reports, <http://recruiting.jobvite.com/resources/reports/> (last visited Oct. 4, 2012).

3. Employers should be aware of the EEOC's current focus on eliminating systemic discrimination, such as discriminatory barriers in recruitment and hiring.

4. 42 USC §2000 ff.

activity<sup>5</sup> can be particularly troublesome. Consider, for example, a hiring employer in a state with such a law finds photos on the applicant's website showing the applicant smoking marijuana and decides not to hire that individual. Certainly, the use of the marijuana can be illegal, but it may not be. The individual could be legally using it for medicinal purposes or using it in a state or country where marijuana is permissible. The material the individual is smoking may not even be marijuana or another illegal substance.

- **Background and Credit History Information.** Making a hiring decision based on an individual's arrest history, conviction<sup>6</sup> or credit history can be problematic under federal and/or state law. For example, the Federal Fair Credit Reporting Act ("FCRA") requires employers to obtain consent before conducting background checks through consumer reporting agencies. This means that employers that engage certain third parties to obtain background information on applicants, such as information concerning reputation, may be required under FCRA to obtain the applicant's written consent. If an employer decides not to hire an applicant based on information in a consumer report obtained from a social networking site through a third party, the employer may be required under the FCRA to notify the applicant that its decision was based on that information.

Federal law also prohibits employers from discriminating against an applicant based on the employee's current or prior filing for bankruptcy. As discussed above, a number of states, likely in response to economic conditions, passed laws that prohibit employers from discriminating against employees and applicants on the basis of credit-related information, such as payment history.

- 
5. See, e.g., Colo. Rev. Stat. Ann. § 24-34-402.5(1); N.D. Cent. Code Ann. § 14-02.4-03, -8; and N.Y. Lab. Law § 201-d.
  6. The EEOC has set parameters on the use of criminal records in hiring and retention decisions. See EEOC Enforcement Guidance, Number 915.002 (April 25, 2012), [http://www.EEOC.Gov/laws/guidance/arrest\\_conviction.cfm](http://www.EEOC.Gov/laws/guidance/arrest_conviction.cfm). In light of the EEOC's Guidance, before disqualifying an individual with a criminal record from employment, employers should engage in an individualized assessment involving a dialogue with that individual. While the Guidance states that employers would not violate federal anti-discrimination law if they disqualify an applicant based on separate federal restrictions on the employment of persons with criminal records, an employer may not defend a decision to qualify an individual solely on state restrictions on the hiring of persons with criminal records. The Guidance also discourages the use of criminal conduct inquiries on employment applications, recommending that such inquiries be addressed later in the employment consideration process.

- **Inaccurate information.** The cliché - *Don't believe everything you read!* – applies not only to information you find in the newspaper. Information obtained online frequently is inaccurate, misleading or not provided in the proper context. Basing a decision on incorrect information not only poses the risk of a lawsuit from the applicant, but even if the applicant does not sue, the company can potentially lose its next star employee. The same can be true for an employee seeking a different position inside the company. In that case, the problems that tainted the hiring process would be likely to also adversely impact the individual's current employment.
- **Impermissibly obtaining access to the information.** Employers must also be cautious in how they go about accessing information available about a job applicant through social media. As discussed above, a number of states have made it illegal to request and/or require employees or applicants to provide the username and passwords necessary to access their Facebook and other social media and online accounts, or created a commission to look at the issue. It also is imperative that employers avoid circumventing a potential employee's privacy settings by pretending to be someone else in order to gain access to a restricted network.<sup>7</sup>

A decision not to hire an individual based on some of the activities described above could result in the individual suing the employer, alleging that the decision was discriminatory or otherwise unlawful. This risk, among other considerations, has caused many employers to stop requiring applicants to submit certain information with their resume or application, as well as to cease searching social networking sites that may reveal sensitive information. Companies that take this approach need to be sure that directive has reached all of the managers and supervisors that are involved in the hiring process as many turn to social media as a matter of course in vetting candidates.

Acquiring the information also poses risks even if the company hires the individual. If the new employee is aware that the company has certain information, such as health-related information (e.g. cancer diagnosis) concerning the employee's spouse, and is later subject to an adverse employment decision, the employee may attribute that decision to the

---

7. See, e.g., *Brian Pietrylo v. Hillstone Rest. Group*, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009) (court refused to overturn jury verdict finding managers accessed a private, invitation-only chat group without authorization in violation of the federal SCA).

information the employer obtained in the hiring process, and not the poor performance the employer claims is the basis of the adverse action.

### **III. EMPLOYEE MONITORING**

There are many reasons companies monitor employees, including boosting productivity, dissuading cyber-slacking or social “not-working,” protecting trade secrets and confidential business information, preventing theft, avoiding data breaches, avoiding wrongful termination lawsuits, ensuring that employees are not improperly snooping themselves, complying with electronic discovery requirements, and generally dissuading improper behavior.

Excessive, clumsy, or improper employee monitoring, however, can cause significant morale problems and, worse, create potentially legal liability for invasion of privacy under statutory and common law. With new technology, there are more methods of monitoring than ever before. Each has different limitations under the law. Here are some examples:

- *Monitoring work email communications.* Pros: generally lawful, effective. Notice requirements exist in some states (e.g. CT, DE).
- *Monitoring internet usage.* Cons: Often misleading, can be expensive.
- *Monitoring social media.* Cons: May violate state law regarding social media passwords or common law.
- *Accessing employee cloud-based internet accounts by accessing and obtaining user name and password from a work computer.* Cons: Likely to violate the federal Stored Communications Act.
- *Tracking employee whereabouts by GPS (either a phone app or vehicle based device).* Cons: Morale issues, may be invasion of privacy. (An employee in CA recently sued and reached a settlement with her employer after she was terminated for uninstalling a company-required 24-hour tracking app in her phone).
- *Tracking employees with a Radio Frequency Identification Device (RFID).* Cons: Expensive, strange, morale issues, some states (WI, ND, MO) explicitly prohibit employers from implanting chips in employees.
- *Motion Sensors.* Cons: The Daily Telegraph, a London-based newspaper, recently reversed a decision to install motion sensors at desks after employees cried Big Brother. (The employer claimed it was just seeking to monitor how many shared desks were used and not used).

- *Video*. Pros: Extremely effective in loss prevention and investigation of bad acts. Cons: Some notice requirements. Avoid cameras in changing areas, locker rooms, etc.
- *Audio*. Pros: Also effective in obtaining and preserving certain types of evidence. State wire-tap laws may apply.
- *Physical searches*. Pros: Sometimes necessary, little or no expense. Cons: May violate common law right of privacy depending on circumstances.
- *Obtaining health or fitness information*. Cons: May violate the Health Information Portability and Accountability (HIPAA), Genetic Information Nondiscrimination Act (GINA) and other laws.
- *Drug testing*. Pros: Workplace safety; Cons: expense, tightly regulated in some states.
- *Polygraphs*. Cons: Restricted by federal law and many states.

We'll focus here on one form of monitoring, reviewing employee email or other electronic communications in transit or stored on the employer's networks or other systems. This is a popular form of employee monitoring engaged in by employers, or vendors on their behalf. Examples of these communications include:

- email correspondence (including content of the email) between employer-provided email accounts, or between an employer-provided email account and a non-employer provided email account;
- personal emails (including content of the emails) to and from a non-employer provided email account (such as Yahoo mail or Gmail) that are accessed using employer information systems, or which are captured through the use of certain software applications (employing, for example, keylogging and screen-shot functionality) and forwarded to the employer;
- instant message communications made using employer-provided or non-employer provided platforms; and
- social media communications captured using screen shots, including communications that might otherwise have been shielded by the employee's privacy settings/password.

The monitoring could employ the following techniques:

- Keylogging, screenshot, spyware software (example: SpectorSoft);
- Real-time monitoring of Instant Messages (example: iTunes if configured for real-time), SMSs, chat rooms, etc.;
- Retrieval of stored exchange email;
- Forensic retrieval of email from returned computers/laptops;
- Review of stored Instant Messages (example: iTunes, Oxygen Forensic); or
- Internet content.

Below is a discussion of some of the key federal statutes regulating these kinds of monitoring activities, with an emphasis on use of spyware technologies.

- **Electronic Communication Privacy Act.** As many commentators and courts have expressed, applying the Electronic Communication Privacy Act (ECPA) is difficult, particularly given the failure of the statutory provisions to keep pace with the rapid advancements in technology. Some courts have nonetheless been faced with the task of applying the ECPA's protections to the kinds of monitoring technologies referenced above, although not always in an employment context. Some of the non-employment cases may, nonetheless, be instructive.

In an effort to summarize some of the key points of the ECPA, note that as a threshold matter, some courts have held that to have standing to make an interception claim under the ECPA, the plaintiff must have a legitimate expectation of privacy in the communications claimed to be intercepted.<sup>8</sup> The analysis of whether there is a legitimate expectation of privacy is two-pronged: (i) did a subjective expectation of privacy exist, and (ii) was there an objectively reasonable expectation of privacy.<sup>9</sup> However, it is not required that the

- 
8. *Clements-Jeffrey v. City of Springfield*, 810 F. Supp. 2d 857 (S. D. Ohio 2011), citing, *U.S. v. Mendoza*, 574 F.2d 1373 (5<sup>th</sup> Cir. 1978). *Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343, \*5 (D. Mass. May 7, 2002) (instructing employees on how to create passwords for various purposes will not necessarily create an expectation of privacy).
  9. A number of circuits have concluded that a person lacks legitimate privacy expectations in Internet subscriber information and in to/from addresses in emails sent



interception obtain valuable information.<sup>10</sup> But it is required that the interception involve the contents, the substance of a particular communication, not personally identifiable information that is automatically generated by the communication, or silent video tapes.<sup>11</sup> A belief by the sender of the communication that the recipient may forward those communications on to third parties will diminish an otherwise reasonable expectation of privacy.<sup>12</sup> Additionally, interceptions must be intentional and not inadvertent.<sup>13</sup>

---

via ISPs. *Rehberg v Paulk*, 611 F.3d 828 (11th Circuit 2010), citing *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (collecting cases from the Fourth, Sixth, and Ninth Circuits and district courts in West Virginia, Massachusetts, Connecticut, Maryland, New York, and Kansas); and *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (“[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their [\*\*28] messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.”). See also *U.S. v. Thomas*, 2013 U.S. Dist. LEXIS 159914 (D. Vt. Nov. 8, 2013) (No reasonable expectation of privacy in downloaded files from peer-to-peer file sharing network.).

10. *U.S. v. Szymuszkiewicz*, 622 F.3d 701, 703 (7th Cir. 2010).
11. *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 2013 U.S. Dist. LEXIS 145727, 2013 WL 5582866 \* 15-17 (D.Del. 2013) (“personally identifiable information that is automatically generated by the communication” is not “contents” for the purposes of the Wiretap Act); citing *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (2012) (data conveying the geolocation was not contents, as it was automatically generated by the iPhone); *Sams v. Yahoo!, Inc.*, No. 10-5897, 2011 U.S. Dist. LEXIS 53202, 2011 WL 1884633, at \*6-7 (N.D. Cal. May 18, 2011) (records identifying persons using Yahoo ID and email address, IP addresses, and login times was not content-based); *In re § 2703(d) Order*, 787 F. Supp. 2d 430, 435-36 (E.D. Va. 2011) (the Wiretap Act did not cover unique Internet Protocol (“IP”) number, Twitter subscriber, user, and screen names, addresses (including e-mail addresses), telephone or instrument number or other subscriber number or identity, and temporarily assigned network address); *U.S. v. Polizzi*, 549 F. Supp. 2d 308, 393 (E.D.N.Y. 2008) (finding in the context of a Fourth Amendment search that “[n]o expectation of privacy exists for other . . . online transactional information, such as a user’s Internet search history”), vacated on other grounds by 564 F.3d 142 (2d Cir. 2009). See also, *Minotty v. Baudo*, 42 So. 3d 824, 830-1 (Fla. Dist. Ct. App. 4th Dist. 2010), citing, *Sanders v. Robert Bosch Corp.*, 38 F.3d 736 (4th Cir. 1994); *People v. Drennan*, 84 Cal.App.4th 1349, 1358 (2000) (Penal Code section 632 does not extend to taking timed, still photographs without accompanying sound); *State v. Jackson*, 650 So. 2d 24 (Fla. 1995) (distinguishing between “tone-only” pagers (not subject to federal and state wiretap protection) and digital display pagers).
12. *Garrity*, 2002 U.S. Dist. LEXIS 8343, \*4.
13. *Hayes v. Spectorsoft Corporation*, 2009 U.S. Dist. LEXIS 102637 (E. D. Tenn. Nov. 3, 2009), citing, *In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 22-23 (1st Cir. 2003).

In a recent class action under ECPA, the plaintiff alleged that the computer she was renting-to-own from defendant had spyware installed on it, which she was not aware of when she leased it.<sup>14</sup> That software product, “PC Rental Agent,” was “invisible and generally undetectable” and permitted the installer to:

*remotely install or build a ‘Detective Mode’ on the RTO computer over the internet ... [allowing] the installer [] to choose the various levels of surveillance [that] permit the installer to secretly take photographs with the RTO computers’ webcams, and capture keystrokes, and screen shots . . . If the rent-to-own store wants [\*4] more information, it can cause Detective Mode to record data every two minutes until prompted to stop doing so. DesignerWare’s servers collect this information and transmit it to the franchisee for however long the franchisee leaves the program turned on.*

The Court found the facts alleged in the complaint were plausible on their face to state an ECPA claim and that, if true, would subject defendants to liability under ECPA for intercepting plaintiff’s private communications. The Court appeared to follow the line of cases holding that an “interception” under the ECPA occurs only when the acquisition is contemporaneous with the transmission.<sup>15</sup> However, the Court stated that “given the sophistication of the technology at issue, it is entirely possible that discovery will reveal that the screenshots, keystrokes and pictures were in some state of “transmission” as envisaged by the statute when they were obtained by PC Rental Agent.

At least two Federal Circuit Courts of Appeal have questioned whether interceptions must be simultaneous with transmission in order to trigger an ECPA violation.<sup>16</sup> The holdings in these cases may

- 
14. *Arrington v. Colortyme, Inc.*, 2013 U.S. Dist. LEXIS 132907 (W. D. Pa Sept. 17, 2013). It is worth noting that no claims appear to have been made under the applicable Pennsylvania statute – a two-party consent state.
  15. *Id.* at 30, citing *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003) (requiring simultaneity of acquisition and transmission of electronic communication) (citing *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (When Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term “intercept” with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make that definition applicable to voice mail messages as well. Congress, therefore, accepted and implicitly approved the judicial definition of “intercept” as acquisition contemporaneous with transmission.”); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994).
  16. *U.S. v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (“electronic communication includes transient electronic storage that is intrinsic to the communication process

be instructive for employers considering the use of more robust monitoring technologies, such as spyware. In *U.S. v. Szymuszkiewicz*, for example, the Seventh Circuit analyzed a feature of Microsoft Outlook that allows all emails received by an Outlook user's account to be forwarded to another Outlook user. In this case, an employee applied this rule to his supervisor's computer without her knowledge. The defendant argued that this was not an interception under the ECPA because his supervisor's emails were forwarded to him only after they arrived on her computer.<sup>17</sup> However, the Court found:

*Either the server in Kansas City or Infusino's computer made copies of the messages for Szymuszkiewicz within a second of each message's arrival and assembly; if both Szymuszkiewicz and Infusino were sitting at their computers at the same time, they would have received each message with no more than an eyeblink in between. That's contemporaneous by any standard. Even if Infusino's computer (rather than the server) was doing the duplication and forwarding, it was effectively acting as just another router, sending packets along to their destination, and Councilman's conclusion that the Wiretap Act applies to messages that reside briefly in the memory of packet-switch routers shows that the Act has been violated.<sup>18</sup>*

The federal district court in the Northern District of California analyzed the ECPA in an employment context in *Brahmana v. Lembo*. In that case, the plaintiff alleged that the employer used software and monitoring tools such as local area network analyzers and keyloggers to obtain the passwords to his personal email account, and ulti-

---

for such communications), citing, *In Re Pharmatrak, Inc.*, 329 F.3d at 21-2 (discussion in dicta as court found acquisition of communication was contemporaneous with transmission); *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010), followed by, *Klumb v. Goan*, 884 F. Supp. 2d 644 (E. D. Tenn. 2012) (In opining on husband's allegations that his former wife's installation of SpectraSoft spyware on his computer was an interception in violation of the ECPA, the court relied on its analysis earlier in the case, "That the e-mail may have rested momentarily in the intended recipient's account before being transmitted back though the internet to the third party is of no consequence. That the recipient and the third-party might access their respective email accounts on the same computer is immaterial. The e-mail has still been captured and rerouted within a "blink of an eye" through the internet to someone who was not authorized to have it. That is contemporaneous enough."). But, see, the dissenting opinion in *Councilman* which argued that every court that passed on this issue previously had found that interceptions do not occur when the communications are in electronic storage, "even if the storage lasts only a few mili-seconds." *Councilman*, 418 F.3d at 87 (dissenting opinion).

17. *Szymuszkiewicz*, 622 F.3d at 703.

18. *Id.* at 706.

mately his email account itself.<sup>19</sup> The court made clear that in the Ninth Circuit access to stored communications will not violate ECPA section 2511<sup>20</sup> and that “interceptions” of electronic communications means acquiring them during transmission.<sup>21</sup> Thus, the court dismissed the ECPA claims concerning the employee’s *stored* personal emails under ECPA section 2511(1)(a).

When analyzing the keylogger technology, the court considered whether keylogging may constitute an electronic transmission. The Northern District looked at the decision in *U.S. v. Ropp*,<sup>22</sup> which considered whether the logging of keystrokes being transmitted between the keyboard and the CPU had to be in interstate commerce or needed only to affect interstate commerce. The *Ropp* court decided that such transmissions did not affect interstate commerce and, therefore, were not actionable under the ECPA. This court appeared to agree that the focus should be on whether the transmitting system *affects* interstate commerce, although it did not resolve whether the transmission must be *traveling* in interstate commerce. Finding the allegations sufficient to state a claim, the court noted that further discovery can help to determine the effect on interstate commerce.

The 11th Circuit addressed a similar issue more recently and, after confirming that “interception[s] of electronic communications must occur contemporaneously with their transmission,” explained that “use of a keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce).”<sup>23</sup> Applying *Barrington* and *Ropp*, the federal district court in *Rene v. G.F. Fishers, Inc.*, held that

*while the Defendants’ keylogger software may have captured transmissions in transit, the system through which these signals traveled did not affect interstate or foreign commerce. As a result, the intercepted keystrokes are not “electronic communications” under the FWA. Because the intercepted keystrokes were not electronic communications, they could not be “intercepted” as that term is defined in the FWA. For this reason the Court accordingly holds that the Defendants’ keylogger software did*

---

19. *Brahmana v. Lembo*, 2009 U. S. Dist. LEXIS 42800 (N.D. Calif. May 20, 2009).

20. *Id.* at 7, citing *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9<sup>th</sup> Cir. 2002).

21. *Id.* at 7. See also *Hernandez v. Path, Inc.*, 2012 U.S. Dist. LEXIS 151035 (N.D. Calif. Oct. 19, 2012).

22. 347 F.Supp.2d 831 (C.D. Cal. 2004).

23. *United States v. Barrington*, 648 F.3d 1178 (11<sup>th</sup> Cir. 2011).

*not intercept an electronic communication as a matter of law, and Rene's claim for interception must fail.*<sup>24</sup>

**Consent exception.** A key exception to an interception claim under the ECPA is consent.<sup>25</sup> In general, consent exists where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights.<sup>26</sup> The *In re Pharmatrak* decision provides a helpful discussion of what constitutes "consent" to support a defense:

*A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications. [citations omitted] "Thus, 'a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.'" [citations omitted] Consent may be explicit or implied, but it must be actual consent rather than constructive consent. [citations omitted] ... Consent "should not casually be inferred." [citations omitted] "Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception." Berry v. Funk, 331 U.S. App. D.C. 62, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation omitted); accord Lanoue, 71 F.3d at 981; see also Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("Knowledge of the capability of monitoring alone cannot be considered implied consent.").*<sup>27</sup>

A number of courts have found, in general, that consent can be implied when an employer's policies concerning the use of its information systems make clear that employees have no expectation of privacy.<sup>28</sup> For example, under a Fourth Amendment analysis involving an employee of the federal government, the following steps taken by the employer undermined the employee's claim of a subjective

---

24. *Rene v. G.F. Fishers, Inc.*, 2011 U.S. Dist. LEXIS 105202 (S.D. Ind. Sept. 16, 2011).

25. ECPA section 2511(2)(d).

26. *Griggs-Ryan v. Smith*, 904 F.2d 112, 116 (1<sup>st</sup> Cir. 1990).

27. *In re Pharmatrak*, 329 F.3d at 23-23, citing, *Griggs-Ryan*. See also *Shefts v. Petrakis*, 2012 U.S. Dist. LEXIS 130542, \*22 (C.D. Ill. 2012) (knowledge of capability of monitoring alone does not constitute implied consent).

28. See also, *Mortensen v. Bresnan Communication*, 2010 U.S. Dist. LEXIS 131419 (D. Mont. December 13, 2010) (in case involving monitoring customer activity on ISP provider's website for preference-sensitive advertising, ECPA claims were dismissed even if plaintiff had subjective expectation of privacy because Online Privacy Statement and OnLine Subscriber Agreement provide notice of monitoring and forwarding of electronic activities to third parties). *Shefts*, 2012 U.S. Dist. LEXIS 130542, \*22 (consent hinges on whether individual has notice of the fact communications would be monitored; employee manual contained clear warnings).

expectation of privacy for personal items stored on government-issued devices:

- express policies notifying all employees that they have no expectation of privacy when they access the DOJ's computer information systems;
- IT manuals and policies reminding employees that there is no expectation of privacy in the use of government computers or computer systems, and, to the extent that employees wish that their private activities remain private, they should avoid using departmental computer systems for such activities;
- policy that provided that use of an employer-provided computer or telecommunications system, including a personal computer connected to the employer's network, constitutes consent to monitoring;
- every time employee logged on to his government-issued computer, he was reminded that he had "no reasonable expectation of privacy regarding any communication transmitted through or data stored on this information system," and that at any time, the government may monitor, intercept, search and/or seize data transmitted or stored on the system; and
- reminders of these policies were provided at annual Computer Security Awareness Training sessions.<sup>29</sup>

Similarly, a Federal district court in the Northern District of California found that implied consent existed under circumstances where the employee was repeatedly informed that the employer monitored the use of computers. In this case, in order to turn on and use the work computer, the employee had to click "OK" to clear a warning notice informing him of the monitoring.<sup>30</sup> Additionally, where an employee agrees to the terms of a company computer use policy, a policy that made clear the company can monitor messages on the computer whether used in the office or at home, the employee will not have a reasonable expectation in the personal use of that computer, even if using it at home.<sup>31</sup>

---

29. *U.S. v. Linder*, 2013 U.S. Dist. LEXIS 18346, \*12-3 (N.D. Ill. Feb. 12, 2013).

30. *Sporer v. UAL Corp.*, 2009 U.S. Dist. LEXIS 76852, \*17-8 (N.D. Cal. 2009).

31. *TBG Ins. Servs. Corp. v. Superior Court*, 96 Cal.App.4th 443, 453 (2002).

The recent ruling in the *In re Google Inc. Gmail Litigation* addressed the issue of implied consent.<sup>32</sup> Initially, the court rejected Google's argument that implied consent exists simply because all email users understand that such interceptions are part and parcel of the email delivery process. Instead the court followed the kind of analysis described above, recognizing the question of implied consent is "an intensely factual question that requires consideration of the circumstances surrounding the interception to divine whether the party whose communication was intercepted was on notice that the communication would be intercepted." The court rejected the plaintiff's argument that those circumstances should only include communications that Google made to them. Rather, the court agreed that a "broad swath of evidence that email users were notified of the interceptions, such as Google disclosures, third-party disclosures, and news articles, are relevant to the factual question of implied consent." Accordingly, the court found the commonality required for class certification was not present given the individual issues concerning consent.

However, careful drafting of employment policies is critical. In an analogous situation, where the issue involved an employee waiver of the attorney client privilege, a court found that an employer's "Computer & Internet Usage Policy" failed to address whether the hard drive of company-issued laptops were private, leaving the employee's expectation of privacy with respect to the hard drive intact.<sup>33</sup> Furthermore, at least one court has found that "knowledge of the capability of monitoring alone cannot be considered implied consent."<sup>34</sup> However, the court in *In re Google Inc. Gmail Litigation* held that a finding of implied consent need not require that email users had specific knowledge of the particular devices that intercepted their emails. "Rather, the fact-finder need only be convinced based on the surrounding circumstances that email users were notified of interceptions."<sup>35</sup>

---

32. *In re Google Inc. Gmail Litig.*, 2014 U.S. Dist. LEXIS 36957 (N.D. Cal. March 18, 2014).

33. *U.S. v. Nagle*, 2010 U.S. Dist. LEXIS 104711 (M.D. Pa. Sept. 30, 2010). See also *Pure Power Boot Camp*, 587 F. Supp. 2d at 559 (employer policy could not provide basis for implied consent to search employee's web-based personal emails because it was limited in its terms to "Company equipment").

34. *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 2013 U.S. Dist. LEXIS 81174, \*21 (N.D. Ohio 2013).

35. *In re Google Inc. Gmail Litig.*, 2014 U.S. Dist. LEXIS 36957, \*78-9 (N.D. Cal. March 18, 2014). Citing *Griggs-Ryan*, 904 F.2d at 117 ("The circumstances relevant

*Service Provider Exception.* Under the ECPA, an officer, employee or agent “of a provider of wire or electronic communication service, whose facilities are used in the transmissions of a wire or electronic communication” will not violate the ECPA by using those facilities “to intercept, disclose or use that communication in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider.”<sup>36</sup> Employers have successfully argued that for the email and similar communication systems they provide to employees, they are considered “providers” under this provision, exempting them from liability for engaging in monitoring of those systems.<sup>37</sup>

Despite these exceptions, the ubiquity of advancing technologies and the ability of more individuals to use that technology creates additional risks for employers. For example, employees may use his or her employer’s systems, as the defendant did in *U.S. v. Szymuszkiewicz*, which could create various issues for the employer, including legal risks and employee relations challenges.

- **Stored Communications Act.** Spyware technologies used to monitor or access certain electronic communications have also created risks under the Stored Communications Act (SCA). In general, the SCA prohibits:

*“intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . or intentionally exceed[ing] an authorization to access that facility . . . thereby obtain[ing]... access to . . . [an] electronic communication while it is in electronic storage . . . .” 18 U.S.C. § 2701(a).*

However, in general, where the employer is the communications service provider, such as through an employer-provided email account, employee emails stored on that system fall within an exception from liability under the SCA.<sup>38</sup>

An issue that arises in SCA cases is whether intentionally accessing personal devices without authorization, such as an employee’s personal laptop or cell phone, would result in an SCA violation. In

---

to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private.”).

36. ECPA section 2511(2)(a)(i).

37. *U.S. v. Mullins*, 992 F.2d 1472 (9<sup>th</sup> Cir. 1993).

38. 18 U.S.C. § 2701(c)(1); *Fraser*, 352 F.3d at 114-5.



*Morgan v. Preston*, plaintiff alleged that his wife installed Spector Pro software on his personal laptop computer and used it to access information and emails stored on the laptop in connection with their personal disputes. This court found, along with a majority of other courts, that an end user computer is not a facility through which an electronic communication service is provided, and therefore does not provide electronic storage within the meaning of the SCA.<sup>39</sup>

- 
39. *Morgan v. Preston*, 2013 U.S. Dist. LEXIS 159641, \*14, n. 3 (M.D. Tenn. November 7, 2013), citing, *See Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 793 (5th Cir. 2012)(a cell phone does not satisfy the SCA’s “electronic communication service” and “electronic storage” requirements); *U.S. v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003)(“hacking into a personal computer to retrieve information stored therein” is not covered by the SCA); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 2013 U.S. Dist. LEXIS 145727, 2013 WL 5582866 \* 7 (D.Del. 2013)(“[a]n individuals personal computing devise is not a ‘facility through an electronic communication service is provided,’ as required under the SCA”); *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1057-58 (N.D. Cal. 2012)(IOS devices such as personal computers are not facilities through which an electronic communication service is provided); *Brooks v. AM Resorts*, 2013 U.S. Dist. LEXIS 93372, 2013 WL 3343993 \*4 (E.D. Pa.)(“no one contests that emails downloaded and stored on a personal computer are not included in the [SCA’s] definition of electronic storage”); *K.F. Jacobsen & Co., Inc. v. Gaylor*, 2013 U.S. Dist. LEXIS 74592, 2013 WL 2318853 \* 5 (D. Or. 2013)(personal “computers are not facilities through which ‘electronic communication services’ are provided”); *International Broth. Of Elec. Workers, Local 134 v. Cunningham*, 2013 U.S. Dist. LEXIS 61083, 2013 WL 1828932 \*4 (N.D. Ill. 2013)(“simply accessing a personal computer to obtain stored data would not run afoul of § 2701”); *Freedom Banc Mortg. Services, Inc. v. O’Harra*, 2012 U.S. Dist. LEXIS 125734, 2012 WL 3862209 \* 9 (S.D. Ohio)(“Information that an individual stores to his or her hard drive, such as images, personal information, and emails that he or she has downloaded, is not electronic storage as defined by the [SCA]”); *Council on American-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F.Supp.2d 311, 337 (D.DC. 2011)(email messages downloaded and stored on, and subsequently accessed solely from a user’s personal computer do not fall within the SCA’s definition of electronic storage); *Pure Power Boot Camp v. Warrior Fitness*.

*Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008)(noting that the “majority of courts which have addressed the issue” have determined that email stored on a personal computer is not subject to the SCA); *Bailey v. Bailey*, 2008 U.S. Dist. LEXIS 8565, 2008 WL 324156 \* 6 (E.D. Mich. 2008)(the SCA “does not extend to emails and messages stored only on Plaintiff’s personal computer”); *In re Pharmatrak, Inc. Privacy Litigation*, 220 F.Supp.2d 4, \*14 (D.Mass. 2002)(a “personal computer is not a ‘facility through which an electronic communication service is provided’ for the purposes of § 2701”)(reversed on other grounds by *Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9 (1<sup>st</sup> Cir. 2003); *Crowley v. CyberSource Corp*, 166 F. Supp. 2d 1263, 1271 (N.D. Cal. 2001)(including a personal computing device within the definition of “facility” rendered other parts of the SCA illogical).

In a variation on these facts, the plaintiff-employee in *Sitton v. Print Direction, Inc.*, brought his personal laptop into work to carry out his sales responsibilities for the company, and connected it to the company's network.<sup>40</sup> When the company learned the employee was competing with it, the employee's manager went into the employee's office, moved the employee's mouse and clicked on and printed the emails that appeared on the screen. It turned out that, unlike in *Morgan*, the emails were not saved to the hard drive of the laptop, but were from a separate email address than the company-provided email – apparently, *a personal web-based email account*.<sup>41</sup>

It is important to note that the court in *Sitton* analyzed the claim under Georgia's Computer Systems and Protection Act, OCGA § 16-9-90, and not the SCA or the ECPA. It found that the employer did not intend to commit the acts prohibited by the Georgia law.<sup>42</sup> It also found that in light of the company's employee manual, the employer had authority to access the laptop, noting that the computer usage policy in the manual was **not** limited to company-owned equipment, but any email "left on or transmitted over these systems."<sup>43</sup> It is unclear whether this rationale would apply, for example, to screenshots of emails spyware might capture.

In *Lazette v. Kulmatycki*, the employee-plaintiff was provided a BlackBerry device by her employer and was told that she could use the device for personal emails.<sup>44</sup> The employee maintained a gmail account that could be accessed from the device, but thought she had deleted the account when she returned it to the company. However, the employee learned some 18 months later that after returning the device Kulmatycki had been reviewing her emails on her gmail account, allegedly 48,000 of them.

In analyzing the plaintiff's SCA claims, the court rejected the employer's argument that because it owned the device, it had authority to access the emails. The court also rejected the employer's argument the BlackBerry was a "facility" and as such the SCA permitted the employer to access the emails. As in *Morgan*, the court found that the BlackBerry was not the facility, instead the g-mail server

---

40. *Sitton v. Print Direction, Inc.*, 2011 Ga. App. LEXIS 849 (Ga. App. Sept. 28, 2011).

41. *Id.* at 4-5.

42. *Id.* at 5-6.

43. *Id.* at 8-9. The court distinguished the decision in *Pure Power Boot Camp v. Warrior Fitness Boot Camp* by claiming a hacking took place in that case, but not here. However that distinction is not entirely persuasive to us.

44. *Lazette*, 2013 U.S. Dist. LEXIS 81174.

was the facility through which the electronic communication service was provided. The court also found that the employee did not implicitly consent to the access because she turned over the BlackBerry without deleting the g-mail account, noting that “[n]egligence is, however, not the same as approval, much less authorization. There is a difference between someone who fails to leave the door locked when going out and one who leaves it open knowing someone be stopping by.”<sup>45</sup>

The court also addressed the issue of whether the emails were in electronic storage, noting that there are two lines of authority. The first is the majority of cases that hold that only emails that are awaiting opening by the intended recipient are in “electronic storage,” and protected under the SCA.<sup>46</sup> The second is the minority of cases that hold that electronic storage includes undeleted emails that have already been opened by the intended recipient. This court chose to follow the majority view. Accordingly, the plaintiff’s SCA claims were permitted to proceed to the extent they related to the emails in the employee’s g-mail account that the employer opened *before* she did.

- **Examples of unintended consequences of information obtained or believed to be obtained through monitoring.** As discussed above, use of certain monitoring technologies to monitor employee communications presents risks under the ECPA, the SCA and other laws. But there are other issues that can arise sometimes unexpectedly when engaging in monitoring. Below are some examples.

**ERISA claims.** In *Alfonso v. Tri-Star Search LLC*, the plaintiff-employee alleged that her employer monitored her electronic communications with her attorney, specifically her Hotmail email account, using a program called “Personal Inspector.” However, in this case, the employee argued that the employer used the information acquired to interfere with her rights under the company’s ERISA-covered

---

45. *Id* at \*19.

46. *Id*, at \*22-3, citing, *In re DoubleClick, Inc. Privacy Litig.*, 154 F.Supp.2d 497, 511-12 (S.D.N.Y. 2001); *Fraser v. Nationwide Mut. Ins. Co.*, 135 F.Supp.2d 623, 635-36 (E.D.Pa.2001); *U.S. v. Weaver*, 636 F.Supp.2d 769, 771 (C.D.Ill. 2009); *Hilderman v. Enea TekSci, Inc.*, 551 F.Supp.2d 1183, 1205 (S.D.Cal. 2008) (“courts have construed subsection (A) as applying to e-mail messages stored on an ISP’s server pending delivery to the recipient, but not e-mail messages remaining on an ISP’s server after delivery.”); *Jennings v. Jennings*, 401 S.C. 1, 736 S.E.2d 242, 245 (S.C. 2012). See also *Councilman*, 418 F.3d at 81.

employee retirement plan, in violation of Section 510 of ERISA.<sup>47</sup> The court found that the employee's managers never used Personal Inspector to capture her email password, or read her Hotmail emails. However, even where the monitoring is permissible, the information obtained may raise other legal risks simply because the company is aware of information obtained.

Attorney client privilege. The "prevailing view is that lawyers and clients may communicate confidential information through unencrypted email with a reasonable expectation of confidentiality and privacy."<sup>48</sup> However, to the extent these technologies and monitoring activities result in access to communications between an employee and his or her attorney, the majority rule is that where the employer maintains and implements a policy that is communicated to employees notifying employees of the employer's monitoring of its information systems, including communications systems, the employee will not have an expectation of privacy in those communications, and will be viewed as having waived the attorney-client privilege.<sup>49</sup>

Protecting company equipment. Spyware technologies also can be used to help locate lost or stolen devices. At least one court has noted that while it may be permissible to use such technologies to report back to the company the computer's IP address or geographical location, delving into the electronic communications of those persons who may have possession of the lost or stolen device will raise ECPA issues.<sup>50</sup>

- 
47. *Alfonso v. Tri-Star Search LLC*, 2009 U.S. Dist. LEXIS 37362 (D. Or May 4, 2009).
48. *In re: Asia Global Crossing, Ltd.*, 322 B.R. at 256. See also, *Holmes*, 191 Cal.App.4th at 1068.
49. *In re: Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (S.D.N.Y. 2005) (often cited four factor test: (1) whether company banned personal or objectionable use of company computer or email; (2) whether company monitored use of company computer or email; (3) whether third parties had a right to access the computer or email; and (4) whether the company notified, or whether the employee was aware of use and monitoring policies); *Goldstein v. Colborne Acquisition Company, LLC*, 2012 U.S. Dist. LEXIS 75743, \*9, (N.D. Ill. 2012); *Geer v. Gilman Corp.*, 2007 U.S. Dist. LEXIS 38852 (D. Conn. Feb. 12, 2007); *Leor Exploration & Prod. LLC v. Aguiar*, 2009 U.S. Dist. LEXIS 87323 (S.D. Fla. Sept. 23, 2009); *Pac. Coast Steel v. Leany*, 2011 U.S. Dist. LEXIS 113849 (D. Nev. Sept. 29, 2011); *Aventa Learning, Inc. v. K12, Inc.*, 830 F.Supp.2d 1083, 1106-1110 (W.D. Wash. 2011); *Holmes v. Petrovich Development Company, LLC*, 191 Cal.App.4th 1047 (2011). But see, *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (2010) (regardless of employer policy, public policy weighs in favor of preserving the privilege).
50. *Clements-Jeffrey v. City of Springfield*, 810 F. Supp. 2d 857 (S. D. Ohio 2011).

National Labor Relations Act and Retaliation. Recent National Labor Relations Board (“NLRB” or “Board”) decisions suggest potential claims against employers under the National Labor Relations Act (“NLRA” or “Act”) based on alleged electronic monitoring of employee information about workplace conditions. As discussed below, for an actionable claim to exist in this regard, there must be a preliminary finding that the employee or employees were engaged in protected concerted activity, explained below.

A separate, but related issue, arises when there is a claim that an employer engaged in unlawful surveillance under NLRA by improperly accessing/monitoring employees’ electronic communications.

*Protected concerted activity.* The NLRA confers rights to all non-management employees, whether unionized or not. These rights are derived from Section 7 of the NLRA. Section 7 provides employees with the right to: (a) form, join or assist labor organizations; (b) refrain from such activities; and (c) participate in activity engaged in for “other mutual aid or protection.” In order to be covered by Section 7, the activity engaged in for “other mutual aid or protection” must be “concerted” and “protected.” For an employee’s action to be “concerted,” he or she must act with, or for the benefit of, other employees. Concerted employee activity ranges from large groups of employees acting together to one employee acting alone in the interest of other employees. Activity is generally “protected” if it pertains to terms and conditions of employment. The following factors must be present to constitute protected concerted activity: (a) two or more employees, or one employee, must be acting on behalf of others; (b) the topic must have some relevance to the interests of fellow employees; and (c) the employee must seek to initiate, induce, or prepare for group action. In other words, an individual protest is not protected. Individualized gripes are not protected under the Act. See Tampa Tribune, 346 NLRB 369, 371-372 (2006). The activity is not concerted if it is carried out by a single employee for his or her own benefit but conduct of a single employee on behalf of others may be considered concerted when engaged in “for mutual aid or protection.” A non-exhaustive list of examples of protected activity include: (a) refusing to work in the face of dangerous working conditions; (b) discussing salary, benefits, or job conditions; (c) disseminating communications that are critical of specific managers or company policies; or (d) improving working conditions through assistance of administrative agencies, courts, or legislators. Nevertheless, employees lose the NLRA’s protection if they engage in the

following non-exclusive list of conduct or behavior: (a) engaging in threats or acts of violence; (b) breaching confidentiality regarding sensitive company information (although not related to wages, hours, and working conditions); (c) making deliberately or maliciously false allegations about the employer; (d) engaging in a partial, or intermittent, strike; or (e) blocking public streets or access to the employer's premises.

*The "Wright Line" test.* To establish a prima facie case of discrimination under the Act, a charging party must show that: (1) he was engaged in union or protected concerted activity; (2) the employer knew about such activity; (3) the employer took adverse employment action against the charging party; and (4) there is a link or nexus between the protected activity and the adverse employment action. See e.g. Wright Line, 251 NLRB 1083 (1980).

There must be more than "mere suspicions" that an employer has knowledge of an employee's purported protected, concerted activity. See Amber Foods, Inc., 338 NLRB 712, 714 (2002) (reversing ALJ's decision that the employer violated the Act where the record was insufficient to support a finding that the employer had knowledge of the employee's union activity and holding that "mere suspicions... cannot substitute for actual or circumstantial proof."); Amcast Automotive of Indiana, Inc., 348 NLRB 836, 839 (2006)(knowledge of union activity "must rest on something more than speculation and conjecture.").

Before determining whether an employer has discriminated against an employee in violation of Section 8(a)(1) or 8(a)(3) of the NLRA, there must be a showing sufficient to support the inference that a charging party's protected activity was a substantial or motivating factor in the alleged adverse employment action. Wright Line, 251 NLRB at 1089.

Pursuant to Wright Line, if a charging party can establish a prima facie case of discrimination, the burden shifts to the employer to prove it would have taken the same action irrespective of whether a charging party engaged in protected activity. These are, of course, fact-intensive inquiries.

*NLRB, monitoring and social media.* Although we have seen no guidance from the Board with respect to accessing a social media site where employees may be discussing terms and conditions of employment, Frontier Telephone, 344 NLRB 1270 (2005), enf'd. on other grounds, 181 Fed. Appx. 85 (2d Cir. 2006) is instructive. There, employees engaged in an organizing campaign and used a Yahoo

website to discuss union issues. Id. at 1275. Several employees were in a work area discussing an accretion issue and asked a supervisor what he thought about the union. In response, the supervisor told employees he was aware of the website (website had been shown to him by another employee). Id.

Subsequently, an unfair labor practice charge was filed based upon an employee's claim that he was intimidated by the supervisor's remark because he thought management could not access the website. Id. Reversing an ALJ, the Board dismissed the allegation on the grounds that there was no way to ensure that all subscribers to the website were employees, employees were not told to maintain secrecy of the website, and employees would reasonably believe that the supervisor learned of the activity through public dissemination by another website subscriber. Id. at 1276. The Board also noted that the employees' campaign had become public knowledge at the worksite. Id. (Note that Member Liebman dissented and would have found a violation based on the supervisor's remark. There is no indication though that Liebman dissented with respect to the legitimacy as to how the information was initially obtained, id. at 1276).

Since Frontier, the Board's Division of Advice has also addressed claims of unlawful surveillance in the social media context. See e.g. Public Service Credit Union, 27-CA-21923 (Div. of Advice Nov. 1, 2011) (no unlawful surveillance where charging party restricted access to his Facebook page to his "'friends,' such that he could not have reasonably concluded that the [e]mployer was directly monitoring his Facebook page. In fact, he correctly concluded that the [e]mployer learned of his Facebook activity from his 'Facebook friends.'"); see also MONOC, 22-CA-29008, 22-CA-29083, 22-CA-29084, 22-CA-29234 (Div. Advice May 5, 2010)(no unlawful surveillance where employer obtained employee's Facebook pages and e-mails from other employees without soliciting this information and advising the employee that "a concerned employee had produced them"); Buel, 11-CA-22936 (Div. Advice July 28, 2011) (no unlawful surveillance where charging party "friended" supervisor, thereby inviting supervisor to view his Facebook page, and there was no evidence the supervisor "was acting at the [e]mployer's direction or was on Facebook for the sole purpose of monitoring employee postings;" Intermountain Specialized Abuse Treatment Center, 27-CA-065577 (Div. Advice Dec. 6, 2011) (same).

Based on Frontier, and the Division of Advice memos described above, a sound argument can be made that periodic viewing by

management of publicly-accessible social media websites – in a way consistent with the ability of other users to gain the same access – is unlikely to constitute unlawful surveillance in violation of the Act. The argument is even stronger where the social media site in question is either promoted by the Union, where an employee directed the company’s management to the site (and there is no privacy restriction subsequently breached by management), or where knowledge of the site (and its contents) is already well-publicized.

At the same time, the company’s management should not actively attempt to access password protected sites or “friend” employees (which might, in effect, breach privacy protections) for the purpose of retrieving union-related communications. Arguably, by ensuring that company management and employees do not become “friends” on Facebook (or other social media sites), a company will be able to minimize any claim that it is making a calculated effort to access a particular employee’s Facebook page to monitor employee postings. See Buel (supervisor likely had greater access than general public because of “friend” status). Instead, a company’s focus should be limited to, as described above, publicly available pages. Of course, as an aside, the company’s management should not report to employees the results of the social media research because to do so could very well give off the impression of unlawful surveillance.

*Advancing technologies.* As to the issue of “web crawling,” certain internet-based search engines perform this exact function – retrieving social media site communications based on search terms entered by a user. Although there have been no Board cases directly addressing this issue, in cases where the information retrieved would already be in the public domain, an argument can be made that the same surveillance analysis described above pertaining to the legality of access would apply. At the same time, there are almost certainly web-based programs which are designed to “hack” into password-protected websites. These programs should not be used.

There is one final point for consideration. There is a possibility that some of the software the company may use might not only be looking at websites and other internet sites, but could also be taking screen shots of activity on the employee’s company-issued computer and personal electronic devices. Therefore, those screen shots could be of activity that is taking place on a social media site behind the employee’s privacy settings. Again, although it does not appear the Board has addressed this specific issue (although the Board might eventually do so in anticipated rulings pertaining to whether employees



have the right to use an employer's electronic equipment for union purposes), it has noted in other contexts that where "employees are conducting their activities openly on or near company premises, open observation of such activities by an employer is not unlawful." Roadway Package System, Inc., 302 NLRB 961 (1991). Moreover, the Board has held that "union representatives and employees who choose to engage in their union activities at an employer's premises should have no cause to complain that management observes them." Hoschton Garment Co., 279 NLRB 565, 567 (1986). Absent out of the ordinary, suspicious, or untoward conduct or circumstances, an employer's mere observation of conspicuous protected concerted activity does not qualify as unlawful surveillance. See e.g. Opryland, 323 NLRB 723, 730 (1997).

Based on this case law, an argument can be made that if employees are on notice that they have no expectation of privacy when using the company's electronic communications equipment, open observation of such activities may not constitute unlawful surveillance.

#### **IV. CALIFORNIA'S DEFINITION OF "REASONABLE SAFEGUARDS" FOR PROTECTING PERSONAL DATA**<sup>51</sup>

In February, California Attorney General, Kamala D. Harris – who has been mentioned as a potential nominee to fill Justice Antonin Scalia's recently vacated seat on the U.S. Supreme Court – issued the California Data Breach Report (Report)<sup>52</sup>. The Report provides an analysis of the data breaches reported to the California AG from 2012-2015.

But 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.

---

51. This section was adapted from an article prepared by Jackson Lewis attorneys: Jason C. Gavejian, Principal, Morristown, NJ and Damon W. Silver, Associate, New York, NY.

52. *California Data Breach Report*, California Attorney General, Kamala D. Harris, February 2016. Available at <https://oag.ca.gov/breachreport2016>.

The Report details that nearly 50 million records of Californians have been breached and the majority of these breaches resulted from security failures. In fact, the Report explains that nearly all of the exploited vulnerabilities, which enabled the breaches, were compromised more than a year after the solution to address the vulnerability was publicly available. According to Ms. Harris, “It is clear that many organizations need to sharpen their security skills, trainings, practices, and procedures to properly protect consumers.”

Malware and hacking, physical breaches, and breaches caused by error have been the three most common types of breaches. Of the three, malware and hacking have been by far the largest source of data breaches, with 90% of all records breached by means of malware and hacking. Physical breaches, resulting from the theft or loss of unencrypted data on electronic devices, were next most common, with health care entities and small businesses most heavily impacted. Breaches caused by error – such as mis-delivery of email and inadvertent exposure of information on the public Internet – ranked third. Government entities made half of all such errors.

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.”<sup>53</sup> 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:

<b>CSC 1</b>	Inventory of Authorized and Unauthorized Devices
<b>CSC 2</b>	Inventory of Authorized and Unauthorized Software
<b>CSC 3</b>	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
<b>CSC 4</b>	Continuous Vulnerability Assessment and Remediation
<b>CSC 5</b>	Controlled Use of Administrative Privileges
<b>CSC 6</b>	Maintenance, Monitoring, and Analysis of Audit Logs

---

53. Cal. Civ. Code § 1798.81.5(b).

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.

While the Report, and California's existing law, are focused on protecting the personal information of California residents, it is important to remember California has continuously been at the forefront of data security legislation. In fact, California was the first state to enact a data breach notification law in 2003, and since that time 46 other states have followed suit. As such, it would not be surprising if other states consider the recommendations in the Report, in particular the minimum standards for reasonable safeguards, and implement similar requirements.

## **V. CONTROLLING EMPLOYEE DATA SECURITY RISKS**

A starting point for understanding workplace privacy and security risks and compliance requirements is to begin looking at some of the statutes and regulations that require companies to safeguard sensitive employee data, as well as protect employee privacy. Below are some examples.

- **Social Security Numbers (SSN) Protections.** A number of states limit the situations in which businesses can acquire, use and disclose individuals' SSNs. For example, in Michigan and Connecticut<sup>54</sup>, 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.<sup>55</sup> In New York, business should have policies to limit access to employee SSNs.<sup>56</sup> Because of how vital SSNs

---

54. Mich. Comp. Laws § 445.82 *et seq.*; and Conn. Gen. Stat. § Sec. 42-471.

55. Utah Stat. Ann. § 34-46-201 *et seq.*

56. N.Y. Gen. Bus. Law §399-dd.

are to individuals and to the commission of 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. A number of states have similar protections.

- **Breach Notification Statutes and Regulations.** Forty seven 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.<sup>57</sup> While many of these statutes appear to apply to consumers, others such as the Massachusetts statute clearly apply to the personal information of employees.<sup>58</sup> Data breach response planning should apply not only to payment card or other consumer data, but to employee data as well. Planning should include steps such as (i) identifying internal personnel to lead the response effort; (ii) lining up potential vendors that would be available on a moment’s notice to assist in the response; (iii) sample communications to employees; and (iv) running a tabletop exercise to see how the plan works.
- **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 bank 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, 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.<sup>59</sup>

Compliance with these laws requires a number of steps, including without limitation, conducting and documenting a risk assessment (and updating those assessments periodically and as business changes dictate), establishing a data classification and access management policy, developing and implementing written administrative, physical

---

57. <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

58. Mass. Gen. Laws § 93H-1 et seq.

59. <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 technical safeguards (aka a “written information security program” or a “WISP”), encryption, and training.

- **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.

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.

- **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.<sup>60</sup> A key procedure in a WISP, therefore, is on that ensure personal data is 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.

---

60. <http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx>.

- **Electronic Monitoring/Eavesdropping Statutes.** 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. Employers cite many legitimate reasons for these activities, including managing workflow, data security and customer care.

Monitoring generally 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.<sup>61</sup> 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. Before engaging in monitoring activities, employers must consider applicable state law, as well as the federal laws discussed below which raise issues about the monitoring itself, but the information obtained in the course of monitoring.

Monitoring employee communications, such as in company-provided email, may turn up 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 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.<sup>62</sup>

Another issue that arises in connection with employee monitoring is that under federal law<sup>63</sup> and in at least ten states<sup>64</sup> computer technicians or information technology workers must report child

---

61. See Delaware and Connecticut. Del. Code § 705, Conn. Gen. Stat. § 31-48d.

62. Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (2010).

63. 18 U.S. Code § 2258A.

64. <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).

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. However, as companies become increasingly more engaged in electronic monitoring activities, it is important to be aware of obligations like these.

- **HIPAA Privacy and Security Rules.** 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 because they 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. Final regulations interpreting these changes were issued on January 25, 2013.

While enforcement had been nearly non-existent when the rules first became effective, the Office for Civil Rights has engaged more



recently in a number of enforcement actions<sup>65</sup>, and is about to enter phase 2 of its audit program.<sup>66</sup>

Employers sponsoring group health plans need to be sure that they have taken all the appropriate compliance steps, as applicable, including conducting a risk assessment, amending plan documents, entering into business associate agreements and training employees.

- **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

---

65. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html>.

66. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html>.

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 HIPAA, GINA, ADA, and FLMA 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. In those situations, third party requests, there are a number of additional issues to consider that are beyond the scope of these materials.

- **Credit Protection/Discrimination Laws.** 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 employee’s personal finances. Employers need to educate managers and supervisors about these requirements and direct them not to use this information in making employment decisions.
- **Social Media Account Access Laws.** It is not uncommon for managers and supervisors to use social media as a source for evaluating a potential applicant or a current employee. In some cases, employers require employees to allow access to their personal social media or other online accounts. At least 16 states have rejected this practice, passing laws prohibiting employers from requesting or requiring employees to provide access to the employees’ social media

or online accounts.<sup>67</sup> As with the credit protection/discrimination laws discussed above, companies need to educate managers and supervisors about requiring or even requesting that employees or applicants provide information to access their online accounts. A simple request could violate the law depending on the state. Of course, some states have exceptions for certain industries and when engaging in certain investigations. It is important to review the applicable state law carefully.

- **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 use photographs of its employees in some of its advertising or customer-facing communications. Without the employee's consent, this could constitute an unlawful appropriation for a commercial purpose. Statutes in California, New York and other states require consent in these situations.

- **Website Privacy Statements.** Electronic applications and onboarding is a growing employment practice where by applicants and current employees can apply for jobs, and if hired, enroll in benefits and complete other administrative requirements. Employers should consider what they communicate to applicants and employees concerning the information they collect during these processes. Currently, there is no specific requirement to post a website privacy statement in connection with e-application and onboarding in the United States.

The California Online Privacy Protection Act requires a website privacy statement for website operators that collect personal information from customers, not employees.<sup>68</sup> Even if the California

---

67. <http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx>.

68. Cal. Bus. And Prof. Code § 22575.

statute is not applicable, website privacy statements are a common practice, but often are not modified to address typical employment issues and company practices. Companies that invite individuals (including current employees) to apply for positions through websites should review the privacy statements on those sites to ensure they reflect the companies' practices concerning that information.

Workplace privacy and security risks go beyond securing employee personal information and intruding on the protected and legitimate privacy rights of employees such as forcing access to their personal social media accounts. News reports of massive hackings and breaches caused by cybercriminals, terror groups or even countries around the world certainly are important and can be unsettling. But, for many organizations, they can distract an employer's attention from significant and perhaps more immediate risks that exist within the workforce of the company. Information technology (IT) departments can do a tremendous, albeit imperfect, job securing the systems from outside intruders. However, relying too heavily on external risks at the expense of those that exist internally can spell disaster for any business. Whether inadvertently or intentionally, employees frequently are the cause of improper uses or disclosures of confidential data, putting the company at risk for a data breach, reputational harm, client distrust and lost business, investigation by federal and state agencies, and litigation.

It is true that no system or set of safeguards is infallible; breaches are going to happen. However, here are some basic steps businesses can take to reduce the risks their own employees present. These steps are not exhaustive, but they are good starting points for discussions about how to avoid inadvertent and intentional activities inside the organization that can cause data privacy or security incidents. A further discussion of legal issues concerning some of these steps is provided below.

- **In-person Training.** The Internet is flush with on-line, "in-the-can" training products. These can be a valuable part of any training and awareness program, particularly for conveying general data privacy and security concepts. But there is no substitute for in-person training about the business' own policies as applied to the day-to-day circumstances, needs and obligations of that particular business. Employees need to ask questions and hear how policies interact with their particular job responsibilities to best understand some of the nuances in the law that drive business practices, contractual obligations, and the risk tolerances of management.

At least one state law suggests more specificity is needed when conducting privacy training. The Texas Medical Records Privacy Act, for example, does not mandate in-person training, but does require training to address “state and federal law concerning protected health information *as necessary and appropriate for the employees to carry out the employees’ duties for the covered entity*.”<sup>69</sup> Making training real, practical and regular is critical, and employees likely would benefit most from such training.

- **Enhance Monitoring**. All the training in the world will not protect an organization from an employee intent on improperly accessing or taking personal or company confidential information. Employees planning to move on might try to take intellectual property or trade secrets with them. Employees in fear of losing their job for poor performance might want to collect evidence for subsequent litigation. Implemented carefully and responsibly, monitoring systems activity can be an excellent tool for helping the organization to mitigate and, in some cases, stop data loss.
- **Manage Devices**. The flood of new and more powerful devices carried by employees is a headache for any Privacy Officer or Chief Information Security Officer. As discussed more fully below, some of the risks could be relieved through careful planning and policies such as (i) limiting which personal devices can access company systems and information, (ii) installing mobile device management software; (iii) limiting which employees should be permitted to use personal devices to access company information and systems, and what should they be permitted to access; and (iv) protecting information on the device when the employee is terminated or purchases a new device.
- **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. In some cases, it may need to have an outside vendor assess the performance of its internal team.

---

69. Texas Health and Safety Code § 181.101.

## NOTES

## NOTES

### 3

## Cloud Computing, SaaS and Outsourcing

Keith Larney  
Bonnie Yeomans  
*CA Technologies*

Michelle Perez  
*Interpublic Group*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.





## A. OVERVIEW OF CLOUD OFFERINGS AND COMPARISON TO OUTSOURCING

### Cloud Offerings

The following are the key models of ‘Cloud’ offerings in the market from least to most comprehensive:

- **Infrastructure as a Service (IaaS)** – The vendor is responsible for processors, storage, networking and customer is responsible for Operating System **layer and up**. Examples include Amazon Web Services, Microsoft Azure, Google, CenturyLink and IBM Softlayer
- **Platform as a Service (PaaS)** – Vendor responsible for servers, storage, networking **up to the OS** and the Customer is responsible for the application layer. Examples include Amazon EC2, Salesforce App Cloud: [Force.Com](https://www.salesforce.com/appcloud/) and Microsoft Azure
- **Software as a Service (SaaS)** – SaaS combines IaaS and PaaS plus the application layer, with no Customer responsibilities at any layer. Examples include Salesforce, Workday, Gmail, etc.

### SaaS Characteristics

Think of SaaS as similar to a utility in its nature. A key differentiator from the earlier application service provider model (ASP) is the advent of multi-tenancy. Below are key elements; however, not every SaaS offering will have each of these characteristics:

- **On Demand – Self Service** – Users can self-provision and scale usage and fees up and down as needed
- **Broad Network Access** – Capabilities are available over a network and accessed by use of heterogeneous client platforms
- **Resource Pooling** – Provider’s computing resources are pooled to serve multiple customers using a multi-tenant model with dynamically provisioned resources
- **Rapid Elasticity** – Capabilities can be rapidly provisioned scaling up and down as necessary based on customer demand
- **Measured Service** – Metering can be used to track use, optimize services and resources similar to a utility
- **Common Service** – all users typically using the same instance of the software, subject to potential configuration

## Traditional Outsourcing

- **Services provided by actual third party resources** rather than a pre-packaged offering
- **Ability to customize** to accommodate customer needs
- **Customer control over data processor** either through contract or ability to direct activity

## Deployment

- **Public Cloud.** Service provider makes resources, such as applications and storage, available to the **general public (outside customer's firewall)** over the Internet. Ex: Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform
- **Private Cloud.** A "private cloud" is **generally behind a Customer's firewall**, having attributes of both on-premises software and taking advantage of some of the advantages of a cloud offering (e.g., cost, deployment, management, etc.).
- **Hybrid Cloud.** Cloud offerings **located both inside and outside a Customer's firewall**. Ex: an organization might use a public cloud service such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data.

## B. BENEFITS AND RISKS OF THE CLOUD

The advantages and disadvantages of SaaS noted below are largely assessed in comparison to the on-premises method of licensing software for use behind the customer's firewall on a perpetual basis. SaaS is almost always provided on a subscription basis.

### Advantages/Opportunities:

- a. **Cost** – reduced for customer due to savings on human capital, physical space, electricity and support. Cost shifts to vendor/provider. This is largely dependent on the SaaS being provided through a multi-tenant distribution model

- b. **Security** – is considered more robust in part because customer environments are often complex and hard to fully control, but vendor dependent
- c. **Maintenance** – is easier for the customer because applications do not need to be installed on each user's computer and vendor can apply updates and upgrades universally and at scale; provided re-writing of customizations is not required
- d. **Reliability** – is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery
- e. **Access** – is much faster. Unit cost for onboarding is very low and getting up and running can be quick. Software is essentially already installed and running. There is no installation or implementation process
- f. **Device and location independence** – improves, enabling users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone, tablet, etc.)

#### **Disadvantages/Risks:**

- a. **Security** – is generally better, but if sensitive personal data is being stored in the cloud, need to make sure vendor has appropriate controls
- b. **Data Localization** – can be an issue in some countries; customers may insist on storing within country even if transfer is legal
- c. **Control of Data** – can be tricky – to ensure data is accurate, breach notice, deletion of data – all should be addressed in contract
- d. **Contractual obligations** – of confidentiality may be an issue. Does your contract prohibit you from sharing customer data with a cloud provider?
- e. **Uniformity of Offering** – may be an issue. SaaS vendors typically cannot customize a multi-tenant, public offering without losing economies of scale and causing issues with upgrades though configuration options may be possible
- f. **Cost Over Time** – may be higher. If a customer would have utilized a perpetual, on-premises licensed product for more than 5 years, cost efficiencies may weigh in favor of the on-premises license

### **C. LAWS AND STANDARDS THAT MAY APPLY TO THE VENDOR OR THE CUSTOMER**

EU Data Protection laws - regulators mostly concerned about transparency and control of personal data

- Directive 95/46
- GDPR (replacing the Directive in May, 2018) - new law now applies directly to processors

U.S. privacy laws focused on personal information:

- FTC Section 5
- State breach notification laws
- Massachusetts: 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth
- Nevada: NRS 603A, Security of Personal Information and SB 227 Amendment
- HIPAA, GLBA, PCI-DSS, etc.

Industry Standards – Security Sources

- ISO/IEC 27018 – contains technical controls tailored to protecting personal data maintained by cloud providers. Created new controls to address current EU data protection laws.
- SSAE 16 - auditing standard for service organizations.

### **D. CONTRACT ISSUES – WHAT’S NEGOTIABLE?**

Prioritization of issues will depend in part on the nature of the SaaS offering. Certain offerings such as a service processing credit card transactions will require more robust standards and perhaps certifications as will SaaS involving the processing of sensitive data. Negotiation may depend on the type of data to be placed into the cloud.

1. **Security/Privacy** – Security is often a customer’s primary concern when considering purchasing SaaS or moving to the Cloud. The vendor’s most reliable assurances around security are often viewing a vendor’s certifications and audit results. Imposing a customer’s security standards by trying to force customer’s policies will not work because a SaaS vendor cannot customize its security across multiple users in a multi-tenant model. Audit rights are sometimes discussed.

Important questions are: who is responsible for different parts of security? And what level of security applies?

2. **Limitation of Liability** - Cloud service agreements typically seek to minimize provider's liability for any loss that arises from the provision of the service. This is in part due to the lower margins on an infrastructure-based service. Vendors will often look to limit liability to a multiple of trailing revenues over a fixed time period due to the fact that SaaS is a subscription-based offering that can be utilized for many years.
3. **Access to Data** – During a force majeure event, defining a recovery point objective for the total amount of data that can be lost based on back-up policy is important. Special arrangements may have to be made to access/recover data after expiration of the contract for portability purposes. This may require obtaining transition services from the vendor.
4. **Privacy** – Largely governed by statutes and regulations. Key issues include: negotiation of breach notification provisions in the event of a security breach exposing personal data, specificity of terms and conditions to types of data. Important questions include: Where is data stored and processed? Are data transfer mechanisms in place?
5. **Service Levels** – Contractually specifying requirements for uptime of the SaaS offering. Typically these are a characteristic of the offering and not negotiated. Force majeure events are a typical carve out from the downtime measure; however, there may sometimes be a Recovery Time Objective in such an event for disaster recovery. Potential defined remedies for SLA breach can include service level credits or the right to terminate the Service. Important questions include: How much down time can you accept? What are your remedies?
6. **Subcontractors** – Ensuring that the cloud provider passes on its obligations to its subcontractors and monitors their compliance; difficulties here can arise in the areas of data privacy, breach notification and IT security controls.

## NOTES

## Hot Issues in Tech Law Litigation

Philip Blum  
*CA Technologies*

Manas Mohapatra  
*Twitter*

Tyler Newby  
*Fenwick & West LLP*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.





## **Topics Addressed**

■ CHALLENGES TO ARTICLE III STANDING.....	5
■ ENFORCEABILITY OF ONLINE CONTRACTS AND ARBITRATION CLAUSES.....	7
■ CHOICE OF LAW IN ONLINE AGREEMENTS .....	14
■ CLASS CERTIFICATION ISSUES.....	15
■ PATENT LITIGATION TRENDS .....	17
■ INTERNATIONAL DISCOVERY DEVELOPMENTS.....	18



## **CHALLENGES TO ARTICLE III STANDING**

- I. Article III: constitutional threshold for bringing suit in *federal* court.
  - a. Plaintiff suffered an injury in fact
  - b. that is fairly traceable to the challenged conduct, and
  - c. that is likely to be redressed by a favorable judicial decision
- II. Injury in fact must be concrete, and actual or certainly impending.
  - a. *Spokeo v. Robins*, 136 S. Ct. 1540, 1549 (2016)
    - Allegations of bare procedural violations of a federal statute, divorced from harm, do not satisfy the “concrete injury” requirement.
    - Standing is not automatic when a federal statute “grants a person a statutory right and purports to authorize that person to sue to vindicate that right.”
- III. Examples of cases finding standing:
  - a. *Matera v. Google, Inc.*, (N.D. Cal. 2016)
    - Denied motion to dismiss class action alleging violations of Electronic Communications Privacy Act (ECPA) and the California Invasion of Privacy Act (CIPA).
    - Held that ECPA and CIPA created statutory rights, the violation of which caused a harm that historically has been recognized by courts as a cognizable injury in fact.
    - Plaintiff suffered an injury in fact
  - b. Data Breach cases alleging theft of personal information:
    - *Galaria, et. al. v. Nationwide Mut. Insur. Co.* (6th Cir. 2016). Potential risk of identity theft and fraud following data theft is sufficiently imminent to justify victim’s mitigation expenses, which are injuries in fact.
    - *Lewert v. P.F. Chang’s China Bistro, Inc.* (7th Cir. 2016). Finding risk of fraud and identity theft from criminal data breach of personal information presented imminent risk of injury.
    - *Remijas v. Neiman Marcus Group, LLC* (7th Cir. 2015) (same).

#### IV. Examples of cases finding no standing:

- a. *Braitberg v. Charter Communications, Inc.*, (8th Cir. 2016)
  - No standing for claim alleging cable company failed to delete plaintiff's records after account termination in violation of Cable Communications Policy Act where Plaintiff alleged no adverse consequences.
- b. *Myers v. Nicolet Rest. of de Pere, LLC* (7th Cir. 2016)
  - No standing for FACTA claim where plaintiff suffered no harm from printing of credit card expiration date on receipt.
- c. *Khan v. Children's Nat'l Health Sys.*, (D. Md. 2016)
  - Court dismissed the state law privacy claims arising out of data breach where plaintiff failed to allege any negative impact from violation.
- d. *Attias v. CareFirst, Inc.*, (D.D.C. 2016)
  - Dismissed class action brought under D.C. Consumer Protection Procedures Act following data breach.
  - "Even if Plaintiffs' rights under applicable consumer protection acts have been violated . . . they have not demonstrated that they have standing to press their claims."

#### V. Key Takeaways

- Purely procedural or technical violations of statutory rights are unlikely to result in Article III standing.
- Data breaches of sensitive personal information that can be used for fraud or ID theft are likely to result in Article III standing.
- Parties will continue to push the limits of "concreteness" of injury for statutory violations and whether harm in data breach cases is "certainly impending" in 2017.

## **ENFORCEMENT OF ONLINE AGREEMENTS & ARBITRATION PROVISIONS**

- I. Current and important issue.
  - a. Growth in use of arbitration provisions in online terms of service post *Concepcion* has led to explosion in cases challenging those provisions.
  - b. *Argument for*: “Clickthrough agreements—which consist of visible notice to the user, an affirmative act by a user and a proper call-to-action saying that the affirmative act manifests assent—are enforceable. Let’s call everything else ‘not a contract’ and never use the ‘-wrap’ suffix again. Done.” - Professor Eric Goldman (<http://blog.ericgoldman.org/archives/2016/07/modified-clickwrap-upheld-in-court-moule-v-ups.htm>)
  - c. Two major issues:
    - i. When do online / mobile app terms of service result in contract formation?
    - ii. How are courts treating unconscionability challenges to online TOS arbitration agreements?
- II. Cases finding no assent:
  - a. *Nguyen v. Barnes & Noble* (9th Cir. 2014)
    - Ninth Circuit affirmed denial of motion to compel arbitration of customer’s complaint concerning attempted product purchase, finding lack of contract formation.
    - Although terms were in close proximity to registration button, they were not sufficiently noticeable to put purchaser on notice.

- Screenshot:

**BARNES & NOBLE** Checkout

**Sign in or Proceed as Guest**

**NEW CUSTOMERS AND GUESTS**  
 You do not need to create an account to place an order. Click "Begin Checkout" to continue.  
 To make future purchases even faster, you will have the option of creating an account during checkout.

EMAIL ADDRESS:

**Begin Checkout**

**RETURNING CUSTOMERS**  
 If you have an account, please sign in for faster checkout.

EMAIL ADDRESS:  [Update email address](#)

PASSWORD: (case sensitive)  [Forgot password?](#)

**Sign In**

Customer Service: 1-800-THE-BOOK  
[Terms of Use, Copyright, and Privacy Policy](#)

[Safe Shopping Guarantee](#)  
 © 1997-2012 BarnesAndNoble.com llc

b. *Nicosia v. Amazon*, (2d Cir. 2016)

- No assent for amended terms of service adding an arbitration clause.
- Only notice to user was statement on purchase page: “by placing your order, you agree to Amazon’s privacy notice and conditions of use.” No other buttons showing assent.
- Screenshot:

9/22/2014 Place Your Order - Amazon.com Checkout

**amazon.com** [Sign In](#) [Shipping & Payments](#) [Gift Options](#) [Place Order](#)

**Review your order**  
 By placing your order, you agree to Amazon.com's privacy notice and conditions of use.

**Shipping address** [Change](#)  
 [Redacted address]

**Payment method** [Change](#)  
 Visa [Redacted Card] [Add Card](#)

**Gift cards & promotional codes**  
 Enter Code  [Apply](#)

**Billing address** [Change](#)  
 Same as shipping address

**Or try Amazon Locker**  
 20 locations near this address

**FREE Two-Day Shipping on this Order**  
 [Redacted] you can save \$5.48 on this order by selecting "FREE Two-Day Shipping with a free trial of Amazon Prime" below.  
[Sign up for a free trial](#)

**Estimated delivery: Sept. 25, 2014 - Sept. 26, 2014**

**Choose a delivery option:**

- ☐ **FREE Two-Day Shipping** with a free trial of Amazon Prime --get it Wednesday, Sept. 24
- ☐ **One-Day Shipping** --get it tomorrow, Sept. 23
- ☐ **Two-Day Shipping** --get it Wednesday, Sept. 24
- ☐ **Standard Shipping** --get it Sept 25 - 26
- ☐ **FREE Shipping** --get it Sept. 26 - Oct. 2

**Place your order**

**Order Summary**

Items: [Redacted]

Shipping & handling: [Redacted]

Total before tax: [Redacted]

Estimated tax to be collected: [Redacted]

Total: [Redacted]

Gift Card: [Redacted]

**Order total:** [Redacted]

How are shipping costs calculated?

- c. *Sgouros v. TransUnion Corp.* (7th Cir. 2016)
  - Declined to enforce website’s arbitration clause that did not give reasonable notice that completion of transaction would be considered assent.
  - No clear statement that purchase was subject to any terms and conditions, including arbitration provision, and disclosures were hidden below the scroll bar.
- d. *Meyer v. Uber Technologies, Inc.*, (S.D.N.Y. 2016)
  - Denied motion to compel arbitration, finding no assent to TOS containing arbitration agreement.
  - Court found hyperlink to the TOS and the phrase “By creating an Uber account, you agree to” were inconspicuous in the mobile device registration process.

### III. Cases finding assent:

- a. *Bekele v. Lyft*, (D. Mass. 2016)
  - Enforced arbitration clause in mobile app click-through agreement with drivers.
  - Full TOS was shown to users on screen.
  - At the bottom of the TOS, the App states “Please agree to the Terms of Service to continue” and the user must click an “I accept” button.
- b. *Cullinane v. Uber Technologies*, (D. Mass. 2016)
  - Enforced arbitration clause in mobile app click-through agreement.
  - Court rejected plaintiff’s argument that the ‘I agree’ button could have represented plaintiff’s agreement to use the service but not to agree to the terms of the arbitration agreement.
- c. *Keena v. Groupon, Inc.*, (W.D. N.C. 2016)
  - Granted motion to compel arbitration clause in online TOS – Registration process required user to enter her name and click a box next to the words “I agree to the Terms of Use and Privacy Statement.”



#### IV. Key Takeaways – Contract Formation

- a. Courts focus on whether the agreement gave the user reasonable notice that by registering or clicking a button, the user is entering a contract.
  - “Browse wrap” agreements are unlikely to ever be enforced.
  - “Click wrap” or “click through” agreements are more likely to be enforced.
  - Link to TOS must be conspicuous.
  - TOS terms should not be “below the fold” on mobile screens.
  - Click through should signal that user is agreeing to terms.
  - Courts are particularly demanding on evidence of assent when the business is attempting to enforce an arbitration agreement.

#### V. Enforcement of Online Arbitration Agreements – Unconscionability

- a. *Tompkins v. 23andMe, Inc.* (9th Cir. 2016)
  - Affirmed order granting motion to compel arbitration based on provision in online TOS that consumer entered to view results of offline testing product.
  - Rejected unconscionability challenges to provisions that:
    - Bi-laterally awarded attorneys’ fees to the prevailing party
    - Required non-prevailing party to pay costs of filing
    - Required disputes to be resolved in San Francisco
    - Carved out IP disputes and
    - Limited limitations period to 1 year
    - Gave business right to unilaterally revise agreement
- b. *Mohamed v. Uber Techs.* (9th Cir. 2016)
  - Reversed district court ruling finding arbitration clauses with drivers unconscionable and compelled arbitration.
  - Broad delegation clause was not rendered unequivocal by language elsewhere in the agreement stating that state and

federal courts in SF had exclusive jurisdiction over disputes.

— . . . *This Arbitration Provision requires all such disputes to be resolved only by an arbitrator through final and binding arbitration and not by way of court or jury trial. Such disputes include without limitation disputes arising out of or relating to interpretation or application of this Arbitration Provision, including the enforceability, revocability or validity of the Arbitration Provision or any portion of the Arbitration Provision.*

- Opt-out provision cured otherwise problematic provisions that failed to apprise drivers of sharing of arbitration fees.
- Unconscionable waiver of private attorney general claims was severable.

c. *Cullinane v. Uber* (D. Mass. 2016)

- Found broad arbitration agreement delegated resolution of unconscionability challenge to arbitrator.
  - *[Parties] agree that any dispute, claim or controversy arising out of or relating to this Agreement or the breach, termination, enforcement, interpretation or validity thereof or the use of the Service or Application (collectively, “Disputes”) will be settled by binding arbitration, except that each party retains the right to bring an individual action in small claims court. . . You acknowledge and agree that you and Company are each waiving the right to a trial by jury or to participate as a plaintiff or class User in any purported class action or representative proceeding.*
- Relief was not illusory because Uber paid all costs of arbitration up to \$75,000.
- Class action waiver did not render arbitration relief illusory.

- d. *Bekele v. Lyft* (D. Mass. 2016)
- Found small size and necessity to scroll on smart phone screen did not render arbitration procedurally unconscionable because it did not result in “unfair surprise.”
  - Arbitration provision in TOS was preceded by all caps: “AGREEMENT TO ARBITRATE ALL DISPUTES AND LEGAL CLAIMS.”
  - Although it appeared on page 21 of 33 page document, there was no evidence that plaintiff was pressured to reading it quickly.
  - Plaintiff had manifested assent to the TOS containing the arbitration clause by clicking “I accept.”
  - Court did not address substantive ability because Massachusetts law requires both substantive and procedural unconscionability to void a contract.
- e. *Moule v. UPS* (E.D. Cal. 2016)
- Arbitration terms were not procedurally accessible because they were easily accessible to the customer and presented in a hyperlinked text following prompt during account creation reading: “By clicking the Yes button, you agree to the UPS Tariff/Terms and Conditions.”
  - Two terms held to be substantively unconscionable:
    - UPS retained unilateral right to amend contract without notice.
    - Confidentiality of arbitration procedures.
  - Court severed unconscionable provisions and enforced the rest.
- f. *Keena v. Groupon, Inc.* (W.D. N.C. 2016)
- Rejected procedural unconscionability challenge to the font size and absence of a printed copy because plaintiff did not allege he did not have access and could not read the agreement.
  - Rejected substantive unconscionability challenges
    - Shortened one-year statute of limitations provision was not so short as to be unreasonable.

- Carve out of IP claims was not unilateral and totally one-sided.
- Costs would not be more than court costs, and Groupon agreed to reimburse costs and fees up to \$10,000 for non-frivolous claims.
- Rejected argument that the benefits were so lopsided as to render relief illusory:
  - Groupon provided consideration for the arbitration agreement by giving up ability to bring non-IP claims in court.

## VI. Key Takeaway – Arbitration Unconscionability

- a. No set formula on provisions that will render an agreement substantively unconscionable, but these don't help:
  - Unilateral right of company to amend agreement without express notice and consent.
  - Unilateral prevailing party attorney's fees provisions.
  - Unilateral IP or equitable claim carve-outs.
  - Private attorney general waivers.
  - Fee sharing or fee shifting of arbitration fees and costs.
- b. Provisions that help avoid unconscionability findings:
  - Clear notice and evidence of consent (see contract formation above).
  - Consumer opt-out period.
  - Commitment of company to pay fees and costs up to ceiling.
  - Parties to be responsible for their own attorneys' fees.
- c. Know your chosen law – does it allow severance of unconscionable provisions?

## **CHOICE OF LAW PROVISIONS IN TERMS OF SERVICE**

### **I. Benefits of Choice of Law Provisions**

- a. *Some* predictability as to applicable law:
  - Courts' familiarity with law if combined with forum selection provision
  - Warranty law
  - Statute of limitations
- b. Added benefit of familiarity of judiciary and jury pool when combined with a forum selection provision.

### **II. Risks of Choice of Law Provisions**

- a. Does not guarantee chosen law will be applied, when other states have a strong public policy interest in applying their laws
  - California & Restatement (Second) of Conflict of Laws § 187:
    - Chosen law applies unless it is contrary to a fundamental public policy of another state, and the other state has a materially greater interest in application of its law.
- b. *In re: Facebook Biometric Information Privacy Litig.*, 2016 WL 2593853 (N.D. Cal. May 5, 2016) (Illinois law protecting privacy of residents' biometric information applied despite California choice of law provision).
- c. May undermine argument against nationwide class certification
  - *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797 (1985): court in a nationwide class action involving state law claims must conduct choice of law analysis.
  - Nationwide class cannot be certified under F.R.C.P. 23(b)(3) where there are material differences in state laws.
    - *Mazza v. American Honda Motor Co.*, 666 F.3d 581 (9th Cir. 2012) (material differences in state consumer protection laws precluded nationwide certification).

- Weaker predominance challenge where the parties contractually agree to application of single state's law.
  - *E.g., Pecover v. Elec. Arts, Inc.*, 633 F. Supp. 2d 976, 978–79 (N.D. Cal. 2009) (California choice of law clause in contracts factored toward application of California to nationwide class)

## **CLASS CERTIFICATION DEVELOPMENTS**

### **I. Introduction**

- a. Challenges to Rule 23(b)(3) predominance (not surprisingly) are the focal issues in class certification in consumer class actions in tech cases.
- b. Rule 23(b)(3) requires the court to find that questions of law or fact common to class members ***predominate over any questions affecting only individual members***, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.
- c. Rule 23(b)(3) is a more rigorous inquiry than the “commonality” requirement under Rule 23(a).

### **II. Example Cases**

- a. *Harris v. comScore*, (N.D. Ill. 2013)
  - Rule 23(b)(3) class certified for case alleging data research company had surreptitiously intercepted Internet users' browsing and Internet usage in violation of Electronic Communications Privacy Act.
  - Court found individual factual issues as to damages did not defeat predominance.
- b. *In re: Gmail Litig.*, (N.D. Cal. 2014)
  - Court denied certification of Rule 23(b)(3) class over Google's alleged scanning of email contents without consent.
  - Individual issues of consent predominated because users would have different interpretations of language in Google's privacy policy and different experiences with whether they saw it.

- c. *In re: Yahoo Mail Litig.* (N.D. Cal. 2015)
  - Court certified Rule 23(b)(2) injunctive relief class for similar allegations about email scanning.
  - No predominance analysis is required for 23(b)(2) classes, and the class met the lower bar of commonality.
- d. *In re Lenovo Adware Litig.* (N.D. Cal. 2016)
  - Alleged Lenovo pre-installed advertising software that allegedly tracked users' browsing activities and had a security flaw.
  - Court certified class of purchasers of laptops, finding commonality of legal and factual issues on Computer Fraud and Abuse Act, California Computer Crime Law, and Trespass to Chattels.
  - Court rejected attacks on commonality based on some users' uninstalling, opting out of the software and favorable reviews of software.
- e. *Baum v. Keystone Mercy Health Plan* (PA Super. Ct. 2016)
  - Appellate court affirmed denial of class certification in case brought under unfair competition law by patients whose personal information was on lost flash drive.
  - Plaintiff was unable to show reliance on statements in privacy policy statements by defendant that it would make sure health information was used correctly.
- f. *In Re Facebook Privacy Litigation* (N.D. Cal. 2016)
  - Alleged FB transmitted users' names and FB user IDs to advertisers in "referrer headers" when users clicked an ad.
  - Class certification denied because individual issues predominated over common ones as to whether referrer ids were transmitted.
    - a. In some instances, users' use of privacy tools stripped information from referrer headers.
    - b. Facebook did not transmit referrer headers uniformly.
    - c. Browser settings sometimes resulted in not sending headers.

- g. *Opperman v. Path, Inc., et al.* (N.D. Cal. 2016)
- Alleged free mobile application developer was liable under California common law tort of intrusion upon seclusion for uploading users' smartphone contacts without notice or consent.
  - Rejected attack on Rule 23(b)(3) predominance of common legal issues by finding California law applied to nationwide class because defendant was based in California and directed conduct from California.
  - Court certified nominal damages class:
    - Rejected certification of “actual damages” based on inherent value of privacy.
    - Rejected plaintiffs' proposed conjoint analysis as means of proving damages on class-wide basis.

### III. Key Takeaways

- a. Choice of law provision in TOS may support Rule 23(b)(3) predominance and commonality.
- b. Language in privacy policy or TOS that can be a basis for arguing consent to a practice may defeat Rule 23(b)(3) predominance.
- c. Statutory damages may help show predominance, but may hurt where discretionary.
- d. Classwide damages models in privacy and data breach cases can present predominance challenges.
- e. Will there be a growth in Rule 23(b)(2) cases to avoid predominance problems?

## **PATENT LITIGATION TRENDS**

### I. What does the data tell us?

- Small decline in volume of case filings from 2015.
  - 2015: Average of 1,456 cases per quarter.
  - 2016: Q1 had 958 cases, Q2 has 1,282 cases.



- Venue:
    - ED Tex. (~37%)
    - Dist. of Del. (~10.5%)
    - C.D. Cal (~6.6%)
    - N.D. Ill (~5.7%)
    - Other (~36.1%)
  - NPEs Trends
    - Overall filing rate dropped year over year by 48%.
    - First part of 2016, top 10 patent plaintiffs (NPEs) file around 18% of all cases.
- II. A few key developments.
- a. *Halo Electronics v. Pulse Electronics Inc.* (S. Ct. 2016):
    - Relaxed the standard for proving willful infringement and making it easier for patent owners to recover enhanced damages.
    - Potentially big impact on dynamics of litigation.
  - b. *Alice* Reversals:
    - Supreme Court held in *Alice* that abstract ideas implemented using a computer are not patentable subject matter.
    - Pendulum appears to be swinging back the other way and more and more software patents are surviving.

## **INTERNATIONAL DISCOVERY DEVELOPMENTS**

- I. Conflict of U.S. Discovery with EU Privacy Law
  - a. Increasingly frequent issue in cross-border litigation.
  - b. Supreme Court has held that foreign law prohibition will not always shield information from discovery in the U.S., and that courts must apply a non-exhaustive, multi-factor balancing test *See Societe Nationale Industrielle Aerospatiale v. U. S. District Court*, 482 U.S. 522, 544 (1987):
    - (1) the importance to the . . . litigation of the documents or other information requested;
    - (2) the degree of specificity of the request;

- (3) whether the information originated in the United States;
- (4) the availability of alternative means of securing the information; and
- (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

## II. Example cases

- a. *BrightEdge Techs., Inc. v. Searchmetrics, GmbH*, (N.D. Cal. 2014)
  - Compelled production of employee emails from German company in patent litigation dispute, rejecting argument that doing so would violate German privacy laws.
  - Found the need for the documents in the case were not outweighed by the German law restrictions.
  - Although German privacy law prohibits transfer of personal data to any jurisdiction that does not provide data protection rules functionally equivalent to the EU, exceptions exist, including for litigation.
  - Party seeking to shield data from production due to foreign country's privacy laws bears the burden of showing production is prohibited.
- b. *Salerno v. Lecia, Inc.*, (W.D.N.Y. 1999)
  - Denied motion to compel personnel files and severance packages of defendant's German national employees as transfers of personal data prohibited by German law and the EU Directive 95/46/EC.

## III. Jurisdictional limits of ECPA warrants

- a. *United States v. Microsoft* (2d Cir. 2016)
  - ECPA search warrants for contents of subscribers' electronic communications are limited to communications stored on computers in the United States.
  - Compare to *In Re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984) and progeny

holding that grand jury subpoenas for business records can request documents located overseas if they are in the possession, custody or control of a U.S. entity.

#### IV. Key Takeaways

- a. When responding to discovery requests for data stored abroad or concerning personal data of EU nationals, litigators need to be aware of foreign jurisdiction's data protection laws.
- b. Parties seeking data from outside the U.S. need to be prepared to demonstrate that such data is covered by an exception in the foreign state's data protection laws.
- c. All U.S. litigators will need to become familiar with the EU's General Data Protection Regulation in 2018.

## NOTES

## NOTES

Brief of *Amici Curiae*, Federal Law Enforcement Officers Association, Association of Prosecuting Attorneys, Inc., and National Sheriffs' Association in Support of the Government, *In re Apple v. FBI*, No. CM 16-10-SP (E.D. Cal. 2016)

Submitted by:  
Joseph V. DeMarco  
*DeVore & DeMarco LLP*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



LOGGED

David LaBahn (State Bar No. 128930)  
**ASSOCIATION OF PROSECUTING ATTORNEYS, INC.**  
1615 L Street NW, Suite 1100  
Washington, D.C. 20036  
Phone: (202) 861-2481  
Email: david.labahn@apainc.com

Joseph V. DeMarco  
Urvashi Sen  
**DEVORE & DEMARCO LLP**  
99 Park Avenue, Suite 1100  
New York, New York 10016  
Phone: (212) 922-9499  
Fax: (212) 922-1799  
Email: jvd@devoredemarco.com  
usen@devoredemarco.com

Attorneys for *Amicus Curiae*  
*Federal Law Enforcement Officers Association, the Association of*  
*Prosecuting Attorneys, Inc., and the National Sheriffs' Association*

**UNITED STATES DISTRICT COURT**  
**CENTRAL DISTRICT OF CALIFORNIA**  
**EASTERN DIVISION**

ED No. CM 16-10-SP

IN THE MATTER OF THE SEARCH  
OF AN APPLE IPHONE SEIZED  
DURING THE EXECUTION OF A  
SEARCH WARRANT ON A BLACK  
LEXIS IS300, CALIFORNIA LICENSE  
PLATE 35KGD203

**BRIEF OF AMICI CURIAE  
FEDERAL LAW ENFORCEMENT  
OFFICERS ASSOCIATION,  
ASSOCIATION OF  
PROSECUTING ATTORNEYS,  
INC., AND NATIONAL SHERIFFS'  
ASSOCIATION IN SUPPORT OF  
THE GOVERNMENT'S MOTION  
TO COMPEL APPLE, INC. TO  
COMPLY WITH THIS COURT'S  
FEBRUARY 16, 2016 ORDER  
COMPELLING ASSISTANCE IN  
SEARCH**

Hearing Date: March 22, 2016  
Hearing Time: 1:00 p.m.  
Courtroom: 3 or 4  
Judge: Hon. Sheri Pym

**COPY**

BRIEF OF AMICI CURIAE FLEOA, APA, AND NSA  
ED No. CM 16-10-SP





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**TABLE OF CONTENTS**

Statement of Interest of *Amici Curiae*.....1

Facts and Summary of the Argument.....3

Argument.....4

    I.    Apple’s Refusal to Provide Reasonable Assistance to the  
          Government Hinders Everyday Law Enforcement and Endangers  
          Public Safety .....4

    II.   A Ruling in Favor of Apple Here Will Have a Chilling Effect on  
          Public Assistance to Law Enforcement .....12

Conclusion.....14

**TABLE OF AUTHORITIES**

**Cases**

*Babington v. Yellow Taxi Corp.*,  
    164 N.E. 726 (N.Y. 1928) ..... 12

*In the Matter of Search of an Apple iPhone Seized During Execution  
of a Search Warrant on a Black Lexus IS300, Cal. License  
Plate 35KGD203*, No. ED 15-0451M, 2016 WL 618401  
(C.D. Cal. Feb. 16, 2016).....3

*Quarles and Butler*,  
    158 U.S. 532 (1895) .....12

*Roviaro v. United States*,  
    353 U.S. 53 (1957) .....12

*State v. Floyd*,  
    584 A.2d 1157 (Conn. 1991).....12

*United States v. New York Telephone Co.*  
    434 U.S. 159 (1977).....12, 13

1	<b>Statutes</b>	
2		
3	28 U.S.C. § 1651.....	13
4	Cal. Penal Code § 150.....	12
5	<b>Other Authorities</b>	
6		
7	Apple Inc., Privacy – Government Information Requests – Apple, http://www.apple.com/privacy/government-information- requests/ (last visited Feb. 29, 2016) .....	10
8		
9	<i>The Encryption Tightrope: Balancing Americans’ Security and Privacy: Hearing Before the H. Judiciary Comm.</i> , 114th Cong. 6 (2016) (written testimony of Cyrus R. Vance, Jr., N.Y. County Dist. Attorney).....	5, 6
10		
11	Lori Hinnant & Karl Ritter, <i>Discarded Cell Phone Led to Paris Attacks Ringleader</i> , Associated Press, Nov. 19, 2015.....	10
12		
13	NEW YORK COUNTY DISTRICT ATTORNEY’S OFFICE, REPORT OF THE MANHATTAN DISTRICT ATTORNEY’S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 9 (Nov. 18, 2015) (“NY DA’s Report”) .....	6, 7, 8, 9, 10
14		
15	NPR, <i>It’s Not Just The iPhone Law Enforcement Wants To Unlock</i> , Feb. 21, 2016, <a href="http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock">http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock</a> (last visited Feb. 25, 2016).....	5
16		
17	Peter Holley, <i>A Locked iPhone May Be the Only Thing Standing Between Police and This Woman’s Killer</i> , Wash. Post, Feb. 26, 2016.....	9
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1                   **STATEMENT OF INTEREST OF *AMICI CURIAE***

2           The Federal Law Enforcement Officers Association (“FLEOA”), a  
3 volunteer organization founded in 1977, is the largest nonpartisan, nonprofit  
4 professional association exclusively representing federal law enforcement officers.  
5 FLEOA represents more than 26,000 uniformed and non-uniformed federal law  
6 enforcement officers from over 65 different agencies. FLEOA is a charter  
7 member of the Department of Homeland Security Federal Law Enforcement  
8 Advisory Board; holds two seats on the Congressional Badge of Bravery Federal  
9 Board; and serves on the Executive Board of the National Law Enforcement  
10 Officers Memorial Fund and the National Law Enforcement Steering Committee.  
11 FLEOA provides a legislative voice for the federal law enforcement community  
12 and monitors legislative and other legal issues that may impact federal law  
13 enforcement officers.

14          The Association of Prosecuting Attorneys, Inc. (“APA”) is a national not-  
15 for-profit organization headquartered in Washington, D.C. and made up of elected  
16 and appointed prosecuting attorneys from throughout the nation. The APA  
17 provides valuable resources such as training and technical assistance to  
18 prosecutors in an effort to develop proactive and innovative prosecutorial  
19 practices that prevent crime, ensure equal justice, and help make our communities  
20 safer. The APA also acts as a global forum for the exchange of ideas, allowing  
21 prosecutors to collaborate with all criminal justice partners, providing timely and  
22 effective technical assistance as well as access to technology for the enhancement  
23 of the prosecutorial function. The APA serves as an advocate for prosecutors on  
24 emerging issues related to the administration of justice and development of  
25 partnerships.

26          Chartered in 1940, the National Sheriffs’ Association (“NSA”) is a  
27 professional association headquartered in Alexandria, Virginia, and dedicated to  
28 serving the Office of Sheriff and its affiliates through police education, police

1 training, and general law enforcement information resources. The NSA represents  
2 thousands of sheriffs, deputies and other law enforcement and public safety  
3 professionals, as well as concerned citizens nationwide. The NSA has provided  
4 programs for sheriffs, their deputies, chiefs of police, and others in the field of  
5 criminal justice in order to enable them to perform their jobs in the best possible  
6 manner and to better serve the people of their cities, counties, or other  
7 jurisdictions. The NSA has worked to forge cooperative relationships with local,  
8 state, and federal criminal justice professionals across the nation to network and  
9 share information about homeland security programs and projects.

10 *Amici* members are called upon on a daily basis to protect and serve the  
11 public by investigating criminal activity and wrongdoing and ensuring that the  
12 individuals responsible for it pay the penalty for their crimes. In order to fulfill  
13 their duties, *Amici* members must have access to all reasonable means of  
14 procuring relevant evidence. In this digital age, data stored on mobile devices has  
15 proven time and again to be critical in assisting law enforcement officers to do  
16 their jobs. *Amici* and their members thus have a strong interest in ensuring that  
17 the Court's February 16, 2016, Order is upheld and enforced.

18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1                                   **FACTS AND SUMMARY OF THE ARGUMENT**

2           This is a case in which this Court issued a February 16, 2016, Order (the  
3 “Order”) directing Apple Inc. (“Apple”) to assist in enabling the government’s  
4 search of the government-owned iPhone 5c used by Syed Rizwan Farook (“the  
5 Terrorist”) by providing “reasonable technical assistance to assist law  
6 enforcement agents in obtaining access to the data” on that device.<sup>1</sup> Apple has  
7 refused to comply with the Order.

8           On February 19, 2016, the government filed a motion to compel Apple to  
9 comply (“Government’s Motion to Compel”)<sup>2</sup>, and, on February 25, 2016, Apple  
10 filed an opposition to that motion and a motion to vacate the Order (“Apple’s  
11 Opposition”).<sup>3</sup> *Amici* respectfully submit this brief in support of the  
12 Government’s Motion to Compel.

13           *Amici* believe that the position Apple has taken is a dangerous one. *First*,  
14 Apple’s refusal to provide assistance has far-reaching public safety ramifications  
15 by making it difficult, and in some cases impossible, for law enforcement to fulfill  
16

17  
18 <sup>1</sup> Order Compelling Apple, Inc. To Assist Agents in Search, *In the Matter of*  
19 *Search of an Apple iPhone Seized During Execution of a Search Warrant on a*  
20 *Black Lexus IS300, Cal. License Plate 35KGD203*, No. ED 15-0451M, 2016 WL  
21 618401, at \*1-2 (C.D. Cal. Feb. 16, 2016).

22 <sup>2</sup> Motion to Compel Apple Inc. To Comply With Court’s February 16, 2016 Order  
23 Compelling Apple to Assist Agents In Its Search, *In the Matter of Search of an*  
24 *Apple iPhone Seized During Execution of a Search Warrant on a Black Lexus*  
25 *IS300, Cal. License Plate 35KGD203*, ED No. CM 16-10 (SP), Dkt. 1 (C.D. Cal.  
26 Feb. 19, 2016).

27 <sup>3</sup> Apple Inc’s Motion To Vacate Order Compelling Apple Inc. To Assist Agents in  
28 Search, And Opposition To Government’s Motion To Compel Assistance, *In the*  
29 *Matter of Search of an Apple iPhone Seized During Execution of a Search*  
30 *Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203*, ED No. CM 16-  
31 10 (SP), Dkt. 16 (C.D. Cal. Feb. 25, 2016).

1 its obligation to investigate crimes, protect the public by bringing criminals to  
2 justice, and enforce the law. *Second*, if Apple were to prevail, the public at large  
3 may itself think twice about cooperating with law enforcement when called upon  
4 to do so.

## 5 6 **ARGUMENT**

### 7 **I. APPLE'S REFUSAL TO PROVIDE REASONABLE** 8 **ASSISTANCE TO THE GOVERNMENT HINDERS** 9 **EVERYDAY LAW ENFORCEMENT AND ENDANGERS** **PUBLIC SAFETY**

10 The Parties have extensively briefed the utility and necessity of searching  
11 the cell phone used by the Terrorist on the day of the attacks in San Bernardino.  
12 Yet beyond the facts of that heinous crime, a ruling which validates Apple's  
13 position in this litigation can only serve to hamper the ability of *Amici* to bring  
14 criminals to justice and justice to victims. To be clear: if Apple can refuse lawful  
15 court orders to reasonably assist law enforcement, public safety *will* suffer.  
16 Crimes *will* go unsolved and criminals *will* go free. Apple's iPhones and iPads  
17 are ubiquitous. They are powerful. They are used by criminals, as well as crime  
18 victims. And, until recently, Apple was willing to assist law enforcement in  
19 executing court orders to search these devices. But Apple has changed course. As  
20 this case illustrates, it has redesigned its iOS operating system to make its  
21 products far harder to search pursuant to a warrant, and in this case decided not to  
22 do what it can to help investigate the Terrorist and his murderous crimes. These  
23 decisions -- decisions made in Apple's boardroom -- are already impeding and  
24 damaging investigations in law enforcement offices around the country. As law  
25 enforcement officials who are sworn to ensure public safety, and to solve crimes,  
26 *Amici* are the first responders, the investigators, the law enforcers and the  
27 prosecutors who, day-in and day-out, must live with Apple's decisions. To *Amici*,

1 this is *not* a theoretical debate. It is as real as a killer gone free, as real as a  
2 pedophile planning for his next prey.

3       The importance of access to evidence found on iPhones, iPads, and similar  
4 devices is emphasized by actual, real world examples undisputed by Apple. For  
5 example, in one big-city district attorney's office *approximately 50%* of the  
6 mobile devices currently recovered during investigations are inaccessible to law  
7 enforcement due to the fact that they are running iOS 8.<sup>4</sup> That percentage will, of  
8 course, only grow as time goes on and newer devices replace older ones. As the  
9 DA in that county put it:

10       In some cases, we can't move at all. We can't establish liability or  
11 responsibility because we can't access the phone. In others, it's  
12 affecting our ability to gather all the evidence that's needed to make  
13 sure that we are making the right judgments. And I think it's very  
14 important for people to understand that a prosecutor's job is to  
15 investigate, get all the information and then make the right judgment  
16 as to whether or not we can go forward. It's also our responsibility to  
17 make sure that we are prosecuting the right people. And when we  
18 don't have access to digital devices, we don't have all the information  
19 that we need to make the best judgment as to how the case should be  
20 handled.<sup>5</sup>

21       Other district attorneys throughout the country have had alarmingly similar  
22 experiences with iPhones running the current operating system. For example, last  
23 year the Harris County (Texas) District Attorney's Office was unable to search  
24

25 <sup>4</sup> See *The Encryption Tightrope: Balancing Americans' Security and Privacy:*  
26 *Hearing Before the H. Judiciary Comm.*, 114th Cong. 6 (2016) (written testimony  
27 of Cyrus R. Vance, Jr., N.Y. County Dist. Attorney) ("Vance Hearing  
Testimony"), at 6.

<sup>5</sup> NPR, *It's Not Just The iPhone Law Enforcement Wants To Unlock*, Feb. 21,  
2016, <http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock> (last visited Feb. 25, 2016).



1 more than 100 encrypted (and therefore inaccessible) Apple devices from cases to  
2 date, including human trafficking, violent street crimes, and sexual assaults. In  
3 2016, the number of inaccessible Apple devices for that office already numbers  
4 eight to ten per month. Similarly, in January and February of this year, the Cook  
5 County (Chicago) State Attorney's office has received 30 encrypted devices it  
6 could not access, and the Connecticut Division of Scientific Services has  
7 encountered 46 encrypted Apple devices in criminal cases, including those  
8 involving child pornography.<sup>6</sup>

9 Actual, real-world cases provide a window into the types of cases at stake  
10 for *Amici*:

- 11 • **Homicide (conviction of guilty):** *People v. Hayes*<sup>7</sup>: The victim was  
12 filming a video using his iPhone when he was shot and killed by the  
13 defendant. Because the iPhone was not passcode-locked, the video,  
14 which captured the shooting, was recovered and admitted into  
15 evidence at trial. The defendant was convicted of murder and  
16 sentenced to 35 years to life.<sup>8</sup>
- 17 • **Homicide (exoneration of innocent):** *People v. Rosario*<sup>9</sup>: A  
18 detective obtained a search warrant and an unlock order for certain  
19 iPhones found at the scene of a homicide. He sent the phones to  
20

21 <sup>6</sup> See Vance Hearing Testimony at 6-7.

22 <sup>7</sup> Indictment Number 4451/12.

23 <sup>8</sup> NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE, REPORT OF THE MANHATTAN  
24 DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY  
25 9 (Nov. 18, 2015),

26 <http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf> (the "NY DA's Report").

27 <sup>9</sup> Indictment Number 1859/10.  
28

Apple, which assisted in extracting data from them. The phone data demonstrated inaccuracies in what investigators initially thought to be the timeline of events, and demonstrated that a particular suspect was not, in fact, involved in the murder. A phone number stored in one of the iPhones was eventually linked to another individual, who later confessed and pled guilty to the killing. He is currently serving a sentence of 17 1/2 years' imprisonment.<sup>10</sup>

- **Child Pornography:** *People v. Hirji*<sup>11</sup>: The defendant was arrested after telling a taxi driver about his interest in having sex with children and showing the driver a child pornography image. Upon searching the defendant's iPhone pursuant to a search warrant, investigators discovered a large number of child pornography images. The defendant was convicted of Promoting a Sexual Performance by a Child.<sup>12</sup>
- **Sex Trafficking:** *People v. Brown*<sup>13</sup>: The defendant directed a sex trafficking operation involving at least four women, using physical violence, threats of force, and psychological manipulation to coerce the women to engage in prostitution. Evidence recovered from defendant's electronic devices contained (a) photographs showing him posing his victims for online prostitution advertisements and showing that he had "branded" multiple women with his nickname;

<sup>10</sup> NY DA's Report at 11.

<sup>11</sup> Supreme Court Information Number 3650/15.

<sup>12</sup> NY DA's Report at 9-10.

<sup>13</sup> Indictment Numbers 865/12, 3908/12, and 3338/13.

1 and (b) text messages between him and several victims confirming  
2 that he had engaged in acts of violence against the testifying witness  
3 and others. The defendant was convicted of multiple counts of sex  
4 trafficking and promoting prostitution and was sentenced to 10-20  
5 years in prison.<sup>14</sup>

- 6 • **Cybercrime and Identity Theft:** *People v. Jacas et al.*<sup>15</sup> and *People*  
7 *v. Brahms et al.*<sup>16</sup>: An iPhone was recovered from a waiter who was  
8 arrested for stealing more than 20 customers' credit card numbers by  
9 surreptitiously swiping the credit cards through a card reader that  
10 stored the credit card number and other data. When the phone was  
11 searched pursuant to a warrant, law enforcement officials discovered  
12 text messages between the waiter and other members of the group  
13 regarding the ring's crimes. Based in large part on information  
14 obtained from the phone, investigators were able to obtain an  
15 eavesdropping warrant, and ultimately arrested a 29-member identity  
16 theft ring, including employees of high-end restaurants who stole  
17 credit card numbers, shoppers who made purchases using counterfeit  
18 credit cards containing the stolen credit card numbers, and managers  
19 who oversaw the operation. The group stole 100 American Express  
20 credit card numbers and property worth over \$1,000,000. All of the  
21 defendants pled guilty, and more than \$1,000,000 in cash and  
22  
23

24 <sup>14</sup> NY DA's Report at 9.

25 <sup>15</sup> Indictment Number 42/12.

26 <sup>16</sup> Indictment Number 5151/11.

merchandise was seized and forfeited.<sup>17</sup>

- **Unlawful Surveillance:** *People v. Lema*<sup>18</sup>: The defendant was arrested for unlawful surveillance after a police officer observed the defendant using his phone to film up women's skirts (*i.e.*, "upskirting"). The defendant consented to a search of his phone, but the passcode he provided did not work. Investigators obtained a search warrant and unlock order for the phone. The phone was sent to Apple, Apple extracted data from the phone, and the phone and data were returned to the prosecutor. Two "upskirting" videos were found on the phone, both filmed on the date of the defendant's arrest. Following the trial, at which both videos were entered into evidence, the defendant was convicted as charged, of two counts of unlawful surveillance.<sup>19</sup>

And in one current investigation in Louisiana, a locked iPhone's text messages and other information on the device may hold the only clues to the murder of a pregnant woman gunned down at the front door of her home.<sup>20</sup> These examples, and many more, prove just how essential evidence recovered from iPhones can be.<sup>21</sup>

<sup>17</sup> NY DA's Report at 10-11.

<sup>18</sup> Indictment Number 4117/13.

<sup>19</sup> NY DA's Report at 11.

<sup>20</sup> See Peter Holley, *A Locked iPhone May Be the Only Thing Standing Between Police and This Woman's Killer*, Wash. Post, Feb. 26, 2016, available at <https://www.washingtonpost.com/news/post-nation/wp/2016/02/26/a-locked-iphone-may-be-the-only-thing-standing-between-police-and-this-womans-killer/>.

<sup>21</sup> *Amici* have additional specific, law-enforcement sensitive examples which it

1 Of course, Apple's decisions also hamper crime *prevention*. Data  
2 successfully retrieved from a cell phone after the November 2015 Paris terrorist  
3 attacks on the Bataclan concert hall, where 89 people were killed, reportedly  
4 allowed French law enforcement officials to track down the alleged ringleader,  
5 who later died in a police raid.<sup>22</sup> This individual was in the process of planning  
6 yet another attack in Europe. And lest there be any doubt about the "value-add"  
7 for criminals by Apple's recent engineering decisions and present litigation  
8 posture, *Amici* are even aware of jailhouse statements by criminals about how the  
9 new iOS encryption is a helpful "feature" for planning and committing crimes.  
10 For example, in 2015, the New York Department of Corrections intercepted a  
11 phone call between an inmate and a friend about Apple's new, impregnable  
12 operating system, during which the inmate stated: "*If our phone is running on the*  
13 *iOS 8 software, they can't open my phone. That might be another gift from*  
14 *God.*"<sup>23</sup> In fact, *Amici* are aware of numerous instances in which criminals who  
15 previously used one time, so-called "throwaway" or "burner" phones, have now  
16 switched to the new iPhones as the "device-of-choice" for their criminal  
17 wrongdoing. Troublingly, Apple *even advertises and promotes* its alleged  
18 inability to help law enforcement search these devices.<sup>24</sup>

19  
20 does not wish to place in the public domain. Should the Court, however, desire  
21 this information, *Amici* will make it available.

22 <sup>22</sup> Lori Hinnant & Karl Ritter, *Discarded Cell Phone Led to Paris Attacks*  
23 *Ringleader*, Associated Press, Nov. 19, 2015, *available at*  
24 [http://bigstory.ap.org/article/47e613d2ad184fe4802fd76de903d4bb/french-leader-](http://bigstory.ap.org/article/47e613d2ad184fe4802fd76de903d4bb/french-leader-extremists-may-strike-chemical-bio-arms)  
25 [extremists-may-strike-chemical-bio-arms](http://bigstory.ap.org/article/47e613d2ad184fe4802fd76de903d4bb/french-leader-extremists-may-strike-chemical-bio-arms).

26 <sup>23</sup> NY DA's Report at 12 (emphasis added).

27 <sup>24</sup> Apple's website states, "On devices running iOS 8 and later versions, your  
28 personal data is placed under the protection of your passcode. For all devices

1 To be sure, Apple has greatly assisted law enforcement in the past, helping  
2 officers to unlock the very phones it is now stating it would offend privacy to help  
3 search. This assistance has been critical in a number of law enforcement cases,  
4 both to prosecute criminals and to exonerate the innocent. In this case, law  
5 enforcement has no alternate means of obtaining the information they are  
6 seeking<sup>25</sup> and the iPhone used by the Terrorist may well be as critical to the  
7 resolution of this case as the devices were in the cases described above.

8 In sum, it is crystal clear that Apple's refusal to provide reasonable  
9 assistance to law enforcement has real world, on-the-ground implications for  
10 federal and state law enforcement officers as they do their daily jobs as well as for  
11 the public they are sworn to protect. In many instances, this assistance is critical  
12 to whether or not law enforcement can bring justice and closure to victims'  
13 families and, in cases such as this one, thwart everyday crime and violence as well  
14 as the ever-growing threat of terrorism across the globe.

15  
16  
17  
18 running iOS 8 and later versions, Apple will not perform iOS data extractions in  
19 response to government search warrants because the files to be extracted are  
20 protected by an encryption key that is tied to the user's passcode, which Apple  
21 does not possess." Apple Inc., Privacy – Government Information Requests –  
Apple, <http://www.apple.com/privacy/government-information-requests/> (last  
visited Feb. 29, 2016).

22 <sup>25</sup> Government's Motion to Compel at 6. It bears noting that although critics of  
23 the Government's position here state that law enforcement should simply rely on  
24 data that can be obtained on iCloud, as one DA has stated, even when criminals  
25 choose to back-up their data on the cloud (and in most cases they do not), data on  
26 an iPhone will not be backed up unless the iPhone is connected to Wifi. See  
27 Vance Hearing Testimony at 4. In this particular case, there are indications that  
28 the iCloud account had not been backed up since October 19, 2015. Moreover,  
Apple itself has stated that it cannot provide data that has been deleted from an  
iCloud account. *Id.*

1           **II. A RULING IN FAVOR OF APPLE HERE WILL HAVE A CHILLING**  
2           **EFFECT ON PUBLIC ASSISTANCE TO LAW ENFORCEMENT**

3           Justice Cardozo, in a 1928 decision while he was still a state court judge,  
4           stated: “[A]s in the days of Edward I, the citizenry may be called upon to enforce  
5           the justice of the state, not faintly and with lagging steps, but honestly and bravely  
6           and with whatever implements and facilities are convenient and at hand.”  
7           *Babington v. Yellow Taxi Corp.*, 164 N.E. 726, 727 (N.Y. 1928). Almost 50 years  
8           later, Justice White echoed Cardozo’s words in the Supreme Court’s landmark  
9           decision, *United States v. New York Telephone Co.*, recognizing that “citizens  
10          have a *duty* to assist in enforcement of the laws.” 434 U.S. 159, 175 n.24 (1977)  
11         (emphasis added); *see also* *Roviaro v. United States*, 353 U.S. 53, 59 (1957)  
12         (recognizing the historic obligation of citizens to assist law enforcement and to  
13         communicate their knowledge of criminal activity to law enforcement officials);  
14         *In re Quarles and Butler*, 158 U.S. 532, 535 (1895) (recognizing the duty of  
15         citizens “to assist in prosecuting, and securing the punishment of, any breach of  
16         the peace of the United States”). Indeed, as one state supreme court recognized:

17                 The basic concept that every citizen can be compelled to assist in the  
18                 pursuit or apprehension of suspected criminals has ancient Saxon  
19                 origins, predating the Norman Conquest . . . . As the responsibility  
20                 for keeping the peace shifted, over the centuries, to sheriffs,  
21                 constables, and eventually to trained professional police departments,  
22                 the power of those law enforcement officials to command the  
23                 assistance of citizens was recognized both in statutes and in the  
24                 common law.

25         *State v. Floyd*, 584 A.2d 1157, 1166 (Conn. 1991) (upholding state statute  
26         requiring citizens to provide reasonable assistance to law enforcement) (internal  
27         citations omitted) (footnotes omitted).<sup>26</sup>

28         <sup>26</sup> *See also* Cal. Penal Code § 150 (making it an offense to “neglect[] or refuse[] to  
join the posse comitatus or power of the county, by neglecting or refusing to aid

1 The reasons supporting this venerable principle continue to be true today.  
2 Especially in this digital age, it is now critical for public safety that technology  
3 companies -- and the citizens that manage them -- cooperate with law  
4 enforcement. As the cases above recognize, this is not the first, nor will it be the  
5 last, time that law enforcement enlists the assistance of citizen-managers of  
6 corporations to help them ensure that the law, the bedrock of our society, is  
7 followed and that our officers have the tools and information necessary to enforce  
8 that law, prevent crime and protect the citizenry.

9 In *New York Telephone Co.*, the Supreme Court used the authority of the  
10 All Writs Act, 28 U.S.C. § 1651(a), to order the phone company to do what it was  
11 plainly able to do to assist the FBI in using its facilities and equipment to  
12 apprehend a group suspected of illegal gambling. *See* 434 U.S. at 172, 174.<sup>27</sup>

14 and assist in taking or arresting any person against whom there may be issued any  
15 process, or by neglecting to aid and assist in retaking any person who, after being  
16 arrested or confined, may have escaped from arrest or imprisonment, or by  
17 neglecting or refusing to aid and assist in preventing any breach of the peace, or  
18 the commission of any criminal offense, being thereto lawfully required” to do so  
by a law enforcement officer or a judge).

19 <sup>27</sup> It bears noting that the request here is even less intrusive than was the case in  
20 *New York Telephone Co.* Here, the data at issue is “at rest” -- static data that  
21 exists on a phone whose owner is aware and supportive of law enforcement’s  
22 efforts to retrieve this data. In *New York Telephone Co.*, the data that was to be  
23 accessed was wiretap data belonging to a group of illegal gamblers who were  
unaware that the most private details of their phone conversations were being  
intercepted in real time by law enforcement.

24 Moreover, even if it were true (which it is not, *see* Government’s Motion to  
25 Compel, *supra* note 2) that this particular request implicates the Fourth  
26 Amendment, it is an integral part of our justice system that law enforcement, with  
27 appropriate authority in the form of a search warrant or court order and under  
court supervision, may intrude upon people’s privacy. For example, with court-  
28 authorized search warrants, law enforcement officers are able to enter people’s



1 Today, this Court has used this same statute to order Apple to do what it is plainly  
2 able to do to assist law enforcement in unlocking a cell phone used by the  
3 Terrorist where permission to unlock the phone has already been granted by the  
4 phone's owner (the San Bernardino County Department of Health, the Terrorist's  
5 employer).<sup>28</sup>

6 In short, law enforcement's request, and this Court's order, is neither new  
7 nor novel. What *is* new is Apple's refusal to comply with this reasonable, court-  
8 ordered request for assistance from law enforcement officials. *Amici* are  
9 concerned that were Apple to prevail in this case, the public at large may question  
10 why they should be called upon to cooperate with law enforcement. In countless  
11 ways, knowable and unknowable, this will hamper *Amici's* ability to detect, deter,  
12 and punish crime.

### 13 CONCLUSION

14 *Amici* agree with the Parties that this is an important case. It implicates  
15 privacy. It implicates security. For many years, Apple has provided crucial and  
16 commendable assistance to law enforcement. It has been a valuable partner to  
17 *Amici* in case after case. Apple has changed course in a single -- but a crucial --  
18 way. It has created technical impediments and has refused to provide assistance  
19 which it plainly can to *Amici's* execution of a court-ordered search. That it has  
20 done so in a case involving ISIS-inspired domestic terrorism is disheartening. If


21  
22 bedrooms to search for contraband; collect health records from medical offices;  
23 and even, under some circumstances, search a criminal suspect's attorney's office.  
24 All implicate privacy and it is hardly self-evident as to why a search of an iPhone  
is somehow "special," as Apple seems to contend.

25  
26 <sup>28</sup> Apple has categorically stated that this Court is "a forum ill-suited to address"  
27 the issues in this case, and that the government should instead be seeking to  
28 amend existing legislation. See Apple's Opposition at 2. This is not the law. See  
Government's Motion to Compel at 21-25.

1 upheld by the Court, however, the effects of its refusal will, for countless  
2 Americans, be truly devastating.

3  
4 DATED: March 2, 2016

ASSOCIATION OF PROSECUTING  
ATTORNEYS, INC.

5  
6  
7 By:   
8 David LaBahn

9 DEVORE & DEMARCO LLP  
10 Joseph V. DeMarco  
Urvashi Sen

11 Attorneys for *Amici Curiae*  
12 *Federal Law Enforcement*  
13 *Officers Association, the Association of*  
14 *Prosecuting Attorneys, Inc. and the*  
15 *National Sheriffs' Association*

16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

## NOTES

6

*U.S. v. Knowles*, No. 16 Cr. 005 (PAE)  
(S.D.N.Y 2016)

Submitted by:  
Joseph V. DeMarco  
*DeVore & DeMarco LLP*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



Approved:

*Kristy J. Greenberg*  
Kristy J. Greenberg  
Assistant United States Attorney



Before: HONORABLE HENRY B. PITMAN  
United States Magistrate Judge  
Southern District of New York

15 MAG 4583

UNITED STATES OF AMERICA

- v. -

ALONZO KNOWLES,  
a/k/a "Jeff Moxey,"

Defendant.

COMPLAINT

DOC # \_\_\_\_\_

Violations of  
17 U.S.C. § 506; 18 U.S.C.  
§§ 1028, 2319

COUNTY OF OFFENSE:  
NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

Michael MacDonald, being duly sworn, deposes and says that he is a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI") and charges as follows:

COUNT ONE  
(Criminal Copyright Infringement)

1. On or about December 21, 2015, in the Southern District of New York and elsewhere, ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, unlawfully, willfully, and knowingly did infringe copyrights for purposes of commercial advantage and private financial gain by the reproduction and distribution, including by electronic means, during a 180-day period, of ten and more copies and phonorecords, of one and more copyrighted works, which had a total retail value of more than \$2,500, to wit, without authorization, KNOWLES distributed copies of 15 copyrighted scripts of movies and television shows, which have not yet been publicly released, to an undercover law enforcement agent in exchange for \$80,000 in New York, New York.

(Title 17, United States Code, Section 506(a)(1)(A) and Title 18, United States Code, Section 2319(b)(1).)

COUNT TWO  
(Identity Theft)

2. From on or about December 15, 2015, up to and including on or about December 21, 2015, in the Southern District of New York and elsewhere, ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, would and did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, knowing that the means of identification belong to another actual person, with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law or a felony under any applicable State or local law, to wit, KNOWLES transferred Social Security numbers, driver's license numbers, a passport number, dates of birth, and a bank account number belonging to other individuals to an undercover law enforcement agent located in New York, New York, which information KNOWLES obtained from gaining unauthorized access to the computers of those individuals, in violation of Title 18, United States Code, Section 1030(a)(2).

(Title 18, United States Code, Section 1028(a)(7).)

\* \* \*

The bases for my knowledge and for the foregoing charges are, in part, as follows:

3. I have been a Special Agent with HSI for approximately eight years. For approximately one year, I have been assigned to the El Dorado Task Force in HSI's New York Field Office, during which I have conducted investigations of computer hacking, money laundering, and white collar fraud. I have received training regarding fraud and computer hacking. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports, records, and other evidence. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

**OVERVIEW OF KNOWLES'S SCHEME TO SELL CELEBRITIES'  
PRIVATE AND CONFIDENTIAL INFORMATION**

4. As set forth below, ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, unlawfully accessed the personal e-mail accounts of numerous individuals in the entertainment, sports and media industries (the "Victims"). From their e-mail accounts, KNOWLES stole copyrighted scripts of movies and television shows that had not yet been publicly released, personal identifying information, such as Social Security numbers, and private sexually explicit photographs and videos.

5. In December 2015, ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, offered to sell the stolen material to an individual who, unbeknownst to KNOWLES, was an undercover law enforcement agent (the "UC"). KNOWLES claimed to the UC that he had "exclusive content" that was "really profitable" and worth "hundreds of thousands of dollars." KNOWLES stated that he obtained the material directly from the Victims without their knowledge, and claimed to be able to acquire additional such material from other celebrities and entertainment, sports, and media industry professionals. KNOWLES showed the UC a list of the e-mail addresses and phone numbers of at least 130 such individuals that he had in his possession.

6. On December 21, 2015, during a meeting with the UC in New York, New York, ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, claimed to use two different methods to gain unlawful access to Victims' e-mail accounts. One method, according to KNOWLES, involved sending a "virus" to the Victim's computer which would enable KNOWLES to access it. The other method involved KNOWLES e-mailing a false notification to the Victim stating that the Victim's e-mail account had been hacked, and asking for the Victim's passcodes. Either way, once KNOWLES had successfully accessed the Victim's e-mail account, KNOWLES, unbeknownst to the Victim, changed the settings in the Victim's e-mail account in order to maintain ongoing access to it. KNOWLES attempted to sell numerous movie and television scripts and personal identifying information that he had unlawfully obtained from the Victims to the UC in exchange for approximately \$80,000, whereupon KNOWLES was arrested.

**KNOWLES'S ATTEMPTS TO SELL STOLEN SCRIPTS  
TO A POPULAR RADIO HOST**

7. From speaking with other law enforcement officers, I learned, in substance and in part, that in early December 2015,



representatives of an American premium cable and satellite television network ("TV Network-1") contacted HSI because they had been informed by the executive producer (the "Executive Producer") of a popular drama television series airing on TV Network-1 ("TV Series-1") that an individual may have obtained unauthorized access to scripts of the upcoming season of TV Series-1. In particular, a popular radio host ("Witness-1") had contacted the Executive Producer because Witness-1 had received an unsolicited offer, by e-mail, from an individual who offered to sell Witness-1 scripts of upcoming episodes of TV Series-1.

8. Based on my conversations with Witness-1 and other law enforcement officers, as well as my review of e-mail messages provided by Witness-1 to law enforcement, I have learned the following, in substance and in part:

a. On or about December 4, 2015, Witness-1 received e-mail messages from a particular e-mail address with the header name "jeff moxey," which was later identified as belonging to and used by ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant (the "Knowles E-mail Account"). In those e-mails, KNOWLES claimed to have "full scripts of episodes 1-6" of an upcoming season of TV Series-1. KNOWLES stated that episode 6 of TV Series-1 is currently being filmed, and claimed that he was "certainly capable of getting the rest of the episodes as they are completed." In an e-mail to the UC, KNOWLES also attached screenshots of certain pages of a script of a yet to be aired episode of TV Series-1 (the "TV Series-1 Script Screenshots"). The TV Series-1 Script Screenshots contained a watermark with the name of a particular actress on TV Series-1 ("Victim-1"). KNOWLES asked Witness-1 if there was an offer to purchase the stolen TV Series-1 scripts in Knowles's possession, and Witness-1 responded that Witness-1 would get back to KNOWLES.

b. On or about December 5, 2015, KNOWLES sent messages from the Knowles E-mail Account to Witness-1's phone number. When Witness-1 asked how KNOWLES obtained Witness-1's phone number, KNOWLES claimed to have gotten it from "some other celebrity phone contacts." KNOWLES claimed to have "exclusive content" "worth hundreds of thousands of dollars." KNOWLES stated that he was "[j]ust trying to make a few dollars of these stuff that I got."

c. On or about December 7, 2015, using the Knowles E-mail Account, KNOWLES sent Witness-1 a .pdf file of a script of an upcoming American comedy movie ("Movie-1"), that is not publicly available.

d. That same day, KNOWLES sent messages from the Knowles E-mail Account to Witness-1's phone number. At the direction of law enforcement, Witness-1 discussed with KNOWLES how much KNOWLES would charge for the TV Series-1 scripts. KNOWLES stated that it would be easy to compile the scripts into a book and sell it before the upcoming season of TV Series-1 aired. KNOWLES suggested that because it is a hit show, Witness-1 could sell 100,000 copies of the book at \$20 each, and make \$2 million. KNOWLES also stated that he would have a script for an upcoming hip hop artist biopic movie ("Movie-2") once it is completed at the end of the month.

e. That same day, at the direction of law enforcement, Witness-1 provided the phone number of the UC to KNOWLES, and stated that the phone number belonged to someone interested in KNOWLES's offer to sell scripts. KNOWLES then placed a call from a phone number (the "Knowles Phone Number") to the UC, and they discussed speaking the next day.

**KNOWLES'S ATTEMPTS TO SELL SCRIPTS, SEXUALLY EXPLICIT MATERIAL AND PERSONAL IDENTIFYING INFORMATION OF OTHERS TO THE UC**

9. Based on my conversations with the UC, and my review of e-mail messages and consensually recorded video calls with the UC made using the "FaceTime" application, I have learned the following, in substance and in part:

a. On December 8, 2015, at the direction of law enforcement, the UC attempted to place a FaceTime video call to the Knowles E-mail Account, but did not receive a response. Shortly thereafter, KNOWLES, using the Knowles E-mail Account, placed a FaceTime video call, which was consensually recorded, to the UC, who was located in New York, New York. Based on my review of this consensually recorded FaceTime video call (the "December 8 Call"), I have learned the following, in substance and in part:

i. KNOWLES claimed to have complete scripts for numerous unreleased, upcoming movies and television shows, including six TV Series-1 scripts.

ii. KNOWLES showed the screen of his laptop to the UC, which contained a list of nineteen .pdf files. During the call, KNOWLES opened the majority of the .pdf files, and he scrolled through each of them. KNOWLES stated that these

scripts were for movies and television shows that had not yet been released to the public.

iii. Several of the scripts had distinctive markings on them:

1. The name of Victim-1 was watermarked on the scripts of TV Series-1.

2. The name of a particular casting director ("Victim-2") was watermarked on a script of a particular American comedy movie ("Movie-3").

3. The name of a particular actress ("Victim-3") was watermarked on a script of a particular American comedy movie ("Movie-4"). KNOWLES zoomed in on the Movie-4 Script, which reflected a copyright dated 2015, with "all rights reserved." KNOWLES stated that casting for Movie-4 was underway, and that Movie-4 was scheduled to be released in 2017.

4. The name of a popular hip hop artist ("Victim-7") was reflected on a script of a new television show ("TV Series-2").

iv. KNOWLES stated that once casting is completed for a movie and KNOWLES finds out who is in the movie, it is "easy" for him to get a script for the movie. KNOWLES claimed that he gets the scripts directly from the actors, but stated that the actors do not give him the scripts, nor does he buy any of the scripts.

v. KNOWLES stated that once casting was done for Movie-2, KNOWLES could get the Movie-2 script.

vi. KNOWLES told the UC to let him know if the UC was interested in obtaining a script of any particular movie. KNOWLES stated that he would "definitely be doing more business with you as I get more things. What else are you interested in? Just movie scripts? Or what else?" When the UC responded by asking what else KNOWLES had to offer, KNOWLES stated that he "just got into it," and that he had not been "exploring the possibilities, but the possibilities are definitely unlimited."

vii. After KNOWLES and the UC negotiated, the UC agreed to pay \$75,000 to KNOWLES for all nineteen scripts that KNOWLES had shown on his laptop to the UC. KNOWLES stated that he understood the material he had to be "really profitable."

viii. The UC asked to meet KNOWLES in person, and KNOWLES stated that he was in the Bahamas. The UC asked KNOWLES if he would fly to the United States to exchange the scripts for cash, and KNOWLES agreed to do so.

b. On or about December 11, 2015, the UC, who was located in New York, New York, placed a consensually recorded video call using the FaceTime application to KNOWLES at the Knowles E-mail Account, during which KNOWLES made the following statements, in sum and substance:

i. KNOWLES would provide the UC with his personal information so that the UC could make his travel arrangements to New York City and pay for incidentals related to this trip.

ii. KNOWLES could provide additional movie scripts, as well as private "sex tapes" of other people. The UC expressed an interest in the sex tapes, and asked KNOWLES to send "a small tidbit" of a sex tape for sale.

iii. In response to the UC's inquiry, KNOWLES stated that he gets things straight from the Victims, and that the Victims have no idea what KNOWLES is doing.

iv. The UC asked if KNOWLES also could obtain the personal information of additional individuals, and KNOWLES stated that he had a list of contact information, and that personal information was the easiest thing for him to get. KNOWLES then showed the UC a document on his laptop with a list of names with phone numbers and/or e-mail addresses of at least approximately 130 celebrities (the "List"). The names and contact information of Victim-1 and another actress from TV Series-1 ("Victim-4") were on the List.

v. In response to a question from the UC, KNOWLES stated that he could get Social Security numbers for a few individuals who keep that information in their personal accounts.

c. Later that same day, on December 11, 2015, in an e-mail from the Knowles E-mail Account to the UC, KNOWLES identified himself as "Alonzo Knowles." KNOWLES provided the Knowles Phone Number, as well as his date of birth, passport number, and Money Gram account number, so that the UC could make travel arrangements for KNOWLES and send KNOWLES money for

incidentals in connection with his trip to the United States to meet with the UC. KNOWLES also stated "I will send you Some of the stuff later around 2am. Thats the best time for me to do what i do."

d. On or about December 12, 2015, KNOWLES sent messages from the Knowles E-mail Account to the UC containing sexually explicit images and a video (the "Victim-6 Sexually Explicit Material") from within the e-mail inbox of another radio host ("Victim-5"). The Victim-6 Sexually Explicit Material had been sent to Victim-5 from a television host and columnist ("Victim-6"). KNOWLES stated that "this is free. This is just a sample of things I can get. I have more stuff along these lines and can get more if you're interested in these kind of stuff. I will hold all the other stuff as insurance to make sure things go smooth with my trip. If things go well we can continue doing business and i will give you access to more things."<sup>1</sup>

e. On December 14, 2015, from the Knowles E-mail Account, KNOWLES told the UC that KNOWLES "can't guarantee you socials because 90% of people hardly post it or send it to anyone but [he] will try." KNOWLES stated that he can get "scripts, pics, private videos and conversations, numbers, drivers license and passport info."

f. On December 15, 2015, KNOWLES used the Knowles E-mail Account to e-mail the UC an image of pages of a passport belonging to a particular movie actor ("Victim-9"), which included, among other things, the passport number and date of birth of Victim-9. KNOWLES also provided the Social Security number, address, e-mail address, and phone number for Victim-9 to the UC. The UC replied that if KNOWLES obtained more of this type of information to bring such information to New York City and they would discuss it.

g. Later that same day, December 15, 2015, in an e-mail from the Knowles E-mail Account, KNOWLES told the UC to "[h]ave some extra cash on hand im willing to accept more than 100,000 if we negotiate pass that because i now got the [Movie-2 script] as well and a few other scripts" to sell to the UC.

---

<sup>1</sup> The names and contact information of both Victim-5 and Victim-6 were on the List.

h. On or about December 18, 2015, in e-mail messages between KNOWLES - using the Knowles E-mail Account - and the UC, KNOWLES referenced a public post of Victim-7 about TV Series-2.<sup>2</sup> KNOWLES stated that he had a script of a yet to be aired episode of TV Series-2 to sell to the UC. KNOWLES also asked if the UC had a limit to what he could spend, as KNOWLES has "a lot of data" and KNOWLES did not want to bring everything as "insurance for a possible next meeting." The UC responded that he did not have a limit, and that the UC did not need to buy everything in one shot.

i. On or about December 19, 2015, in an e-mail from the Knowles E-mail Account, KNOWLES told the UC that he had "a very popular A list celebrity ssn along with 30 unreleased tracks towards their upcoming album."

10. Based on my conversations with the UC, and my review of consensually recorded video and audio recordings of a meeting in New York, New York, between the UC and ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, on December 21, 2015, I have learned the following, in substance and in part:

a. KNOWLES provided 15 scripts of television shows and movies which have not yet aired (together, the "December 21 Scripts") to the UC. Among the December 21 Scripts were (i) six scripts of episodes of TV Series-1; (ii) one Movie-1 script; (iii) one Movie-3 script; (iv) one Movie-4 script; and (v) one TV Series-2 script. KNOWLES showed one Movie-2 script to the UC, but did not provide it to the UC.

b. KNOWLES provided Social Security numbers for three professional athletes and Victim-3. For one of the professional athletes ("Athlete-1"), KNOWLES provided the UC with a copy of Athlete-1's form of enrollment in a professional sports league, which contained Athlete-1's Social Security number. For Victim-3, KNOWLES provided the UC with an IRS Notice sent to Victim-3, which contained Victim-3's Social Security number.

c. KNOWLES played an unreleased track of an upcoming album of a popular singer-songwriter ("Victim-8"). KNOWLES noted that Victim-8's music videos had a lot of views on Youtube.

---

<sup>2</sup> The name and contact information of Victim-7 was on the List.

d. The UC asked KNOWLES to demonstrate that KNOWLES can obtain unauthorized access to another individual's personal account. KNOWLES replied that there were two problems, the first being that KNOWLES did not "have [his] VPN<sup>3</sup> so they can track back to your IP Address."<sup>4</sup>

e. KNOWLES identified the second problem as his "social engineering" process, which entails him doing "research on a target." If KNOWLES is "going after a high profile celebrity," then "it is pretty hard to get them." So KNOWLES will "go after" celebrities' friends, whom he finds in pictures with the celebrities. KNOWLES will "hack" the friends of celebrities and "go through their shit" in order to find the phone number of a celebrity. Then, KNOWLES will "hack the celebrity."

f. KNOWLES described two ways in which he gained unauthorized access to celebrities' e-mail accounts. In the first way, KNOWLES will obtain the celebrity's e-mail address, "get their stuff, and [KNOWLES will] basically send them a fake text message making it seem like their account has been hacked. So they write [KNOWLES] back the code [i.e., password] so [KNOWLES] can access it."<sup>5</sup> Once KNOWLES accesses the celebrity's

---

<sup>3</sup> Based on my training and experience, I know that a VPN (virtual private network) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the increased privacy and security of the private network.

<sup>4</sup> Based on my training and experience, I know that an IP Address (Internet Protocol address) is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. A device's IP address can be used to determine its physical location and, thereby, its user.

<sup>5</sup> Based on my training and experience, I believe that KNOWLES is describing a type of "E-mail phishing scam," which is a scheme designed to deceive recipients into divulging private information. E-mail phishing scams typically involve fraudulent e-mail messages appearing to come from a legitimate source in order to trick individuals into responding with private

e-mail account, he changes the "recovery options." The UC asked whether that involves KNOWLES making changes to the celebrity's information so that KNOWLES knows the answer to their security questions, and KNOWLES responded: "yes, exactly."<sup>6</sup> KNOWLES further explained that, in order to avoid detection, KNOWLES deleted notifications from the celebrity's e-mail service provider regarding changes to the settings of the celebrity's e-mail account.

g. The second way that KNOWLES gained unauthorized access to celebrities' e-mail accounts is if KNOWLES has "access to their computer" which is "way easier." If the celebrities have a computer with a Windows operating system, KNOWLES "can just send them a virus and get in that way."

h. The UC handed \$80,000 in cash to KNOWLES for the December 21 Scripts. KNOWLES and the UC agreed that KNOWLES would pay for the Social Security numbers he had provided to the UC next time. After KNOWLES accepted the cash, KNOWLES was arrested.

**KNOWLES DID NOT HAVE AUTHORIZATION TO ACCESS VICTIMS'  
COPYRIGHTED MATERIALS AND PERSONAL INFORMATION**

**TV SERIES-1**

11. Based on my conversations with Victim-1, as well as my review of certain contents of Victim-1's phone and e-mail accounts, I have learned the following, in substance and in part:

a. Victim-1 is an actress on TV Series-1, and is currently filming TV Series-1. The upcoming season of TV Series-1 is set to air in 2016.

---

information (e.g., passwords). Criminals may then use this private information to access the e-mail accounts belonging to other individuals.

<sup>6</sup> Based on my training and experience, I know that, generally speaking, if a user is unable to access his e-mail account, e-mail service providers have "recovery options" which allow users to recover information, such as usernames and passwords, in order to gain access to their e-mail accounts. Typically, a user must answer security questions correctly in order to obtain the username or password for an e-mail account.



b. Victim-1 did not provide any of Victim-1's TV Series-1 scripts to anyone else, nor was she aware of anyone having access to Victim-1's TV Series-1 scripts.

c. In or about September 2015, Victim-1's phone account information was compromised.

d. In or about early December 2015, suspicious activity was detected in Victim-1's e-mail accounts ("Victim-1 E-mail Account-1" and "Victim-1 E-mail Account-2") and Victim-1's Apple account, the latter of which contained a list of Victim-1's passwords to various accounts, including Victim-1's e-mail accounts.

e. Victim-1 provided to law enforcement information from the service provider for the Victim-1 E-mail Account-1. Based on my review of that information, it appears that on or about December 3, 2015, Victim-1's phone was accessed from a location in the Bahamas on or about December 3, 2015 at 2:29 a.m.

f. Prior to this suspicious activity in December 2015, Victim-1 had been receiving TV Series-1 scripts on the Victim-1 E-mail Account-2, and those scripts were watermarked with Victim-1's name on them.

12. Based on my conversations with Victim-4, I have learned the following, in substance and in part:

a. Victim-4 is an actress on TV Series-1.

b. Victim-4 did not provide any of Victim-4's TV Series-1 scripts to anyone else, nor was she aware of anyone having access to Victim-4's TV Series-1 scripts.

c. In or about September 2015, Victim-4's phone account information was compromised. Also during the same time period, suspicious activity involving the use of Victim-4's Social Security number without Victim-4's knowledge or consent was detected in connection with Victim-4's PayPal account.

13. Based on my conversations with employees at TV Network-1, I have learned the following, in substance and in part:

a. The six TV Series-1 scripts offered for sale by ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, are protected by copyright.

b. No one other than the individual whose name is watermarked on the TV Series-1 episode script is authorized to possess the script. It is prohibited to make copies of the TV Series-1 scripts, as they are not for public dissemination, and their secrecy prior to the airing of each episode is significant to the success of TV Series-1.

TV SERIES-2

14. Based on my conversations with employees at another television network ("TV Network-2"), I have learned the following, in substance and in part:

a. The TV Series-2 script offered for sale by ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, is copyrighted.

b. No one other than the individual whose name is watermarked on the TV Series-2 script is authorized to possess the script. It is prohibited to make copies of the TV Series-2 script, as it is not for public dissemination, and the secrecy of the script prior to the public release of TV Series-2 is significant to its success.

MOVIE 1 AND MOVIE-3

15. Based on my conversations with Victim-2, I have learned the following, in substance and in part:

a. Victim-2 was a casting director for Movie-3.

b. Victim-2's Movie-3 scripts had Victim-2's name watermarked on them, and Victim-2 received Movie-3 scripts via e-mail.

c. Victim-2 did not provide any of Victim-2's Movie-3 scripts to anyone else, nor was Victim-2 aware of anyone having access to Victim-2's Movie-3 scripts.

16. Based on my conversations with employees at the particular movie studio responsible for producing Movie-1 and Movie-3 ("Studio-1"), I have learned the following, in substance and in part:

a. The Movie-1 script offered for sale by ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, is protected by copyright.

b. The Movie-3 script offered for sale by KNOWLES is protected by copyright.

c. For both Movie-1 and Movie-3, no one other than the individual whose name is watermarked on the movie script is authorized to possess the script. It is prohibited to make copies of the scripts of Movie-1 and Movie-3, as they are not for public dissemination, and the secrecy of the scripts prior to the public release of Movie-1 and Movie-3 is significant to their success.

#### MOVIE-4

17. Based on my conversations with Victim-3, I have learned the following, in substance and in part:

a. Victim-3 was an actress in Movie-4.

b. Victim-3's Movie-4 scripts had Victim-3's name watermarked on them, and Victim-3 received Movie-4 scripts via e-mail.

c. Victim-3 did not provide any of Victim-3's Movie-4 scripts to anyone else, nor was Victim-3 aware of anyone having access to Victim-3's Movie-4 scripts.

d. Over the last week, suspicious activity was detected in Victim-3's Apple account.

18. Based on my conversations with employees at a movie studio ("Studio-2"), which is responsible for producing Movie-4, I have learned the following, in substance and in part:

a. The Movie-4 script offered for sale by ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, is copyrighted.

b. No one other than the individual whose name is watermarked on the movie script is authorized to possess the script. It is prohibited to make copies of the Movie-4 script, as it is not for public dissemination, and the secrecy of the script prior to the public release of Movie-4 is significant to its success.

**THE VICTIM-6 SEXUALLY EXPLICIT MATERIAL**

19. Based on my conversations with Victim-5, I have learned the following, in substance and in part:

a. Victim-5 had received communications via e-mail from Victim-6.

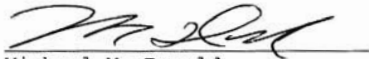
b. Victim-5 did not share with or send to anyone else any sexually explicit material involving Victim-6.

20. Based on my conversations with Victim-6, I have learned the following, in substance and in part:

a. Victim-6 sent the Victim-6 Sexually Explicit Material to Victim-5 via e-mail.

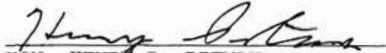
b. Victim-6 did not send the Victim-6 Sexually Explicit Material to anyone else, nor did Victim-6 authorize anyone else to possess, access or send it.

WHEREFORE, I respectfully request that ALONZO KNOWLES, a/k/a "Jeff Moxey," the defendant, be arrested and imprisoned or bailed, as the case may be.



Michael MacDonald  
Special Agent  
Homeland Security Investigations

Sworn to before me this  
22nd day of December 2015



HON. HENRY B. PITMAN  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v.-

ALONZO KNOWLES,  
a/k/a "Jeff Moxey,"

Defendant.

CONSENT PRELIMINARY ORDER OF  
FORFEITURE AS TO SPECIFIC  
PROPERTY/MONEY JUDGMENT

16 Cr. 005 (PAE).

WHEREAS, on or about January 5, 2016, ALONZO KNOWLES, a/k/a "Jeff Moxey" (the "defendant"), was charged in a two-count Indictment, 16 Cr. 005 (PAE) (the "Indictment"), with criminal copyright infringement, in violation of Title 17, United States Code, Section 506(a)(1)(A) and Title 18, United States Code, Section 2319(b)(1) (Count One); and identity theft, in violation of Title 18, United States Code, Section 1028(a)(7) (Count Two);

WHEREAS, the Indictment included a forfeiture allegation as to Count One of the Indictment, seeking to forfeit to the United States, pursuant to Title 18, United States Code, Section 2323(b), all articles made or trafficked as part of the commission of the offense; and all property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of the offense, including, but not limited to, United States currency representing the amount of proceeds obtained directly or indirectly as a result of the commission of the offense alleged in Count One of the Indictment;

WHEREAS, the Indictment included a second forfeiture allegation as to Count Two of the Indictment, seeking to forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1028(b), all property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense and all personal property used or intended to be used

to commit the offense, including, but not limited to, United States currency representing the amount of proceeds obtained directly or indirectly as a result of the offense alleged in Count Two of the Indictment;

WHEREAS, on May 9, 2016, the defendant pled guilty to Counts One and Two of the Indictment, pursuant to a plea agreement with the Government, wherein the defendant admitted the forfeiture allegations with respect to Counts One and Two of the Indictment, and agreed to forfeit to the United States, pursuant to Title 18, United States Code, Sections 2323(b), 982(a)(2)(B) and 1028(b), all articles made or trafficked as part of the commission of the offenses alleged in Counts One and Two of the Indictment; all property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of said offenses; and all property used, or intended to be used, in any manner or part to commit or facilitate the commission of such offenses, including but not limited to a sum in United States currency representing the amount of proceeds obtained as a result of the offense, (the "Money Judgment"); and (ii) all right, title and interest of the defendant in the following specific property seized by Homeland Security Investigations from the defendant: (a) all copies of 25 unpublished television and movie scripts located in the defendant's account with Dropbox, Inc.; (b) all copies of unpublished music located in the defendant's account with Dropbox, Inc.; and (c) 1 Apple iPad mini 1 with serial number F4LK241VF193;

WHEREAS, the defendant consents to the entry of a money judgment in the amount of \$1,982.71 in United States currency;

WHEREAS, the defendant consents to the forfeiture to the United States all of his right, title and interest in the following seized by Homeland Security Investigations from the defendant:

(a) all copies of any original creative content (including but not limited to unpublished movie scripts, unpublished television scripts, and unpublished music) located in the defendant's accounts with the following providers: (1) Dropbox, Inc., (2) Google, Inc., and (3) Microsoft;

(b) all copies of personal identification information of others (including but not limited to names, addresses, Social Security numbers, bank account numbers, Passport numbers, dates of birth, phone numbers, e-mail addresses, visual images and voices) located in the defendant's accounts with the following providers: (1) Dropbox, Inc., (2) Google, Inc., and (3) Microsoft;

(c) all copies of sexually explicit content of others (including but not limited to e-mail messages, visual images, and videos) located in the defendant's accounts with the following providers: (1) Dropbox, Inc., (2) Google, Inc., and (3) Microsoft;

(d) 1 Apple iPad mini 1 with serial number F4LK241VF193;

(e) 1 white Samsung GTS3350 phone with IMEI 351908/05/075125/3  
((a) through (e) collectively the "Specific Property");

WHEREAS, the Government maintains that the following property in the defendant's or an agent of the defendant's custody or control located in the Bahamas (the "Bahamas Property") is subject to forfeiture as a result of the offenses charged in Counts One and Two of the Indictment, to which the defendant pled guilty: (i) all property used, or intended to be



used, in any manner or part to commit or facilitate the commission of criminal copyright infringement, identity theft and computer hacking offenses, including, but not limited to any desktop or laptop computers, tablets, cell phones, external hard drives or electronic storage devices ("Electronic Devices"); and (ii) all property, including but not limited to Electronic Devices, containing the following material: all copyrighted material (original creative content for which the copyright need not have been registered or noticed, including but not limited to scripts of movies and television shows and music that had not yet been publicly released at the time that Knowles obtained it); personal identification information of others (including but not limited to addresses, Social Security numbers, bank account numbers, Passport numbers, dates of birth, phone numbers, e-mail addresses, usernames, passwords, Security questions and answers, access codes, visual images and voices); and sexually explicit material of others (including but not limited to e-mail messages, visual images, and videos), (collectively, the "Stolen Material");

WHEREAS, the defendant represents that no person other than the defendant can claim an interest in the Bahamas Property; and

WHEREAS, the Government and the defendant have agreed to dispose of the Bahamas Property as set forth below, in lieu of forfeiture said property;

IT IS HEREBY STIPULATED AND AGREED, by and between the United States of America, by its attorney Preet Bharara, United States Attorney, Assistant United States Kristy J. Greenberg, of counsel, and the defendant, and his counsel, Clay Kaminsky, Esq., that:

1. As a result of the offenses charged in Counts One and Two of the Indictment, to which the defendant pled guilty, a money judgment in the amount of \$1,982.71 in United States currency (the "Money Judgment") shall be entered against the defendant.

2. As a result of the offenses charged in Counts One and Two of the Indictment, to which the defendant pled guilty, all of the defendant's right, title and interest in the Specific Property is hereby forfeited to the United States.

3. Pursuant to Rule 32.2(b)(4) of the Federal Rules of Criminal Procedure, this Consent Preliminary Order of Forfeiture as to Specific Property/Money Judgment is final as to the defendant ALONZO KNOWLES, a/k/a "Jeff Moxey" upon entry of this Consent Preliminary Order of Forfeiture/Money Judgment, and shall be deemed part of the sentence of the defendant, and shall be included in the judgment of convictions therewith.

4. All payments on the outstanding money judgment shall be made by postal money order, bank or certified check, made payable, in this instance, the United States Customs and Border Protection, and delivered by mail to the United States Attorney's Office, Southern District of New York, Attn: Money Laundering and Asset Forfeiture Unit, One St. Andrew's Plaza, New York, New York 10007 and shall indicate the defendant's name and case number.

5. Upon entry of this Consent Preliminary Order of Forfeiture as to Specific Property/Money Judgment, and pursuant to Title 21, United States Code, Section 853, United States Customs and Border Protection, or its designee the Office of Fines, Penalties, and Forfeitures shall be authorized to deposit the payment on the Money Judgment in the Treasury Assets Forfeiture Fund, and the United States shall have clear title to such forfeited property.

6. Upon entry of this Consent Preliminary Order of Forfeiture as to Specific Property/ Money Judgment, the United States Customs and Border Protection or its designee, shall be authorized to seize the Specific Property and hold the Specific Property in its secure, custody and control, and the United States shall have clear title to such forfeited property.

7. Pursuant to Title 21, United States Code, Section 853(n)(1), Rule 32.2(b)(6) of the Federal Rules of Criminal Procedure, and Rules G(4)(a)(iv)(C) and G(5)(a)(ii) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, the United States shall publish for at least thirty (30) consecutive days on the official government internet forfeiture site, [www.forfeiture.gov](http://www.forfeiture.gov), notice of this Consent Preliminary Order of Forfeiture as to Specific Property/Money Judgment. Any person, other than the defendant in this case, claiming an interest in the Specific Property must file a petition within sixty (60) days from the first day of publication of the notice on this official government internet site, or no later than thirty-five (35) days from the mailing of actual notice, whichever is earlier.

8. This notice shall state that the petition shall be for a hearing to adjudicate the validity of the petitioner's alleged interest in the Specific Property, shall be signed by the petitioner under penalty of perjury, and shall set forth the nature and extent of the petitioner's right, title and interest in the Specific Property and any additional facts supporting the petitioner's claim and the relief sought, pursuant to Title 21, United States Code, Section 853(n).

9. Pursuant to Rule 32.2(b)(6)(A) of the Federal Rules of Criminal Procedure, the Government shall send notice to any person who reasonably appears to be a potential claimant with standing to contest the forfeiture in the ancillary proceeding.

10. Upon adjudication of all third-party interests, this Court will enter a Final Order of Forfeiture with respect to the Specific Property pursuant to Title 21, United States Code, Section 853(n) and Rule 32.2(c)(2) of the Federal Rules of Criminal Procedure, in which all third-party interests will be addressed.

11. Pursuant to Rule 32.2(b)(3) of the Federal Rules of Criminal Procedure, upon entry of this Consent Preliminary Order of Forfeiture as to Specific Property/Money

Judgment, the United States Attorney's Office is authorized to conduct any discovery needed to identify, locate or dispose of forfeitable property, including depositions, interrogatories, requests for production of documents and the issuance of subpoenas, pursuant to Rule 45 of the Federal Rules of Civil Procedure.

12. The defendant shall provide any and all of the Bahamas Property to a receiver appointed by the Court (the "Receiver") no later than one week from the date that this order is entered. The defendant also shall provide a sworn affidavit to the Court, the Receiver, and the Government that he has provided any and all of the Bahamas Property, as described in this Order, to the Receiver, with a brief description for identification purposes (i.e., the make, model and serial number of a particular electronic device) of each item of the Bahamas Property provided to the Receiver no later than one week from the date that this order is entered.

13. The defendant shall relinquish all right, title and interest to the entirety of the Bahamas Property, including the entirety of all Electronic Devices and Stolen Material.

14. The Receiver is hereby authorized to hold the Bahamas Property in its secure custody and control pending a review of its contents in order to confirm that it contains Stolen Material. In particular, the Receiver shall review any laptop computer to confirm whether: (i) its appearance and contents are consistent with the laptop computer that can be seen in the defendant's video teleconference calls with the undercover agent in this case; and (ii) it contains Stolen Material. The Receiver's review of the Bahamas Property, and any and all materials provided to and/or generated by the Receiver, will be governed by the terms of the Protective Order in this case.

15. The Government shall provide to the Receiver any requested materials from the case that would assist in the Receiver's review of the Bahamas Property for the presence of Stolen Material.

16. The Receiver's review of the Bahamas Property shall be completed prior to the defendant's sentencing in this case. In advance of the defendant's sentencing, the Receiver shall provide to the Court, the Government, and counsel for the defendant the Receiver's findings regarding whether: (i) the Bahamas Property contains Stolen Material; and (ii) any of the Bahamas Property is consistent with the above-described video teleconference calls.

17. Upon confirmation that any of the Bahamas Property contains Stolen Material, the Receiver shall promptly destroy the relevant Bahamas Property in its entirety, together with any and all copies thereof, which destruction the Receiver shall verify in writing to the Court and the parties. None of the Bahamas Property found to contain any Stolen Material shall be returned to the defendant or shared with the Government. If any of the Bahamas Property does not contain Stolen Material, the Receiver shall seek guidance from the Court and the parties as to whether any further examination of the property, along with any additional materials from the parties to assist in the Receiver's assessment, is warranted. If the Receiver ultimately determines that property does not contain Stolen Material, the Receiver shall so notify the Court and the parties as described above, and any such property shall be returned to the defendant's counsel.

18. The Government shall not seek to seize, search or forfeit the Bahamas Property that the defendant provides to the Receiver. However, nothing in this Order prevents the Government from seeking to identify, locate, seize, search and forfeit any and all property located in the Bahamas that contains Stolen Material obtained by the defendant that the defendant

does not provide to the Receiver in accordance with this Order, if any such property exists. Moreover, if the Government were to identify any property located in the Bahamas that contains Stolen Material that the defendant obtained but did not provide to the Receiver, nothing in this Order would prevent the Government from bringing otherwise applicable criminal or civil charges against the defendant relating to such Stolen Material.

19. The Court's oral order of September 22, 2016, which restrained the defendant and any of his agents from, among other things, copying, distributing, transferring, moving, or tampering with the Bahamas Property, is hereby amended to permit the defendant through his counsel and any other of the defendant's agents to provide the Bahamas Property to the Receiver, as contemplated by this Order. The Court's restraining order to the defendant and his agents shall otherwise remain in effect until further order of the Court.

20. The Court shall retain jurisdiction to enforce this Consent Preliminary Order of Forfeiture as to Specific Property/Money Judgment, and to amend it as necessary, pursuant to Rule 32.2(e) of the Federal Rules of Criminal Procedure.

21. The Clerk of the Court shall forward three certified copies of this Consent Preliminary Order of Forfeiture as to Specific Property/Money Judgment to Assistant United States Attorney Jason Cowley, Chief of the Money Laundering and Asset Forfeiture Unit, United States Attorney's Office, One St. Andrew's Plaza, New York, New York 10007.

[SPACE INTENTIONALLY LEFT BLANK]

22. The signature page of this Consent Preliminary Order of Forfeiture as to Specific Property/Money Judgment may be executed in one or more counterparts, each of which will be deemed an original but all of which together will constitute one and the same instrument.

AGREED AND CONSENTED TO:

PREET BHARARA  
United States Attorney for the  
Southern District of New York

By: Kristy J. Greenberg  
KRISTY J. GREENBERG  
Assistant United States Attorney  
One Saint Andrew's Plaza  
New York, New York 10007  
(212) 637-2469

9/26/2016  
DATE

ALONZO KNOWLES,  
a/k/a "Jeff Moxey"  
Defendant

By: Alonzo Knowles  
ALONZO KNOWLES

9/26/2016  
DATE

By: Clay H. Kaminsky  
CLAY KAMINSKY, ESQ.  
Federal Defenders of New York, Inc.  
52 Duane St, 10<sup>th</sup> Floor  
New York, New York 10007  
Email: Clay\_Kaminsky@fd.org

9/26/2016  
DATE

SO ORDERED:

Paul A. Engelmayer  
HONORABLE PAUL A. ENGELMAYER  
UNITED STATES DISTRICT JUDGE

9/30/16  
DATE

**Federal Defenders  
OF NEW YORK, INC.**

Southern District  
52 Duane Street-10th Floor, New York, NY 10007  
Tel: (212) 417-8700 Fax: (212) 571-0392

*David E. Patton*  
Executive Director  
and Attorney-in-Chief

*Southern District of New York*  
*Jennifer L. Brown*  
Attorney-in-Charge

November 21, 2016

**BY ECF AND EMAIL**

Hon. Paul A. Engelmayer  
United States District Court  
Southern District of New York  
40 Foley Square, Room 2201  
New York, NY 10007

**Re: United States v. Alonzo Knowles,**  
**16 Cr. 5 (PAE)**

Dear Judge Engelmayer:

I write jointly on behalf of both parties in response to the Court's Order of November 18, 2016.

First, it is the joint position of the parties that the Court should now authorize and direct the Receiver to destroy the laptop and all copies of the materials from it that are in his possession or the possession of the personnel with whom he worked.

Second, the parties also agree that the Court may now set a firm sentencing date for Mr. Knowles. Both parties are available at the Court's convenience on November 30, December 6 until 2:00 p.m., December 7, December 8 until 3:00 p.m., and December 9 before 11:00 a.m.

We thank the Court for its attention to this matter.

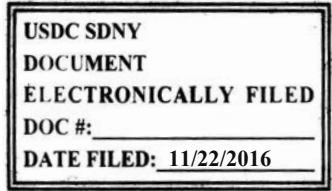
Respectfully submitted,

/s/  
Clay H. Kaminsky  
Assistant Federal Defender  
(212) 417-8749

cc: AUSA Kristy J. Greenberg







UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-v-

ALONZO KNOWLES,

Defendant.

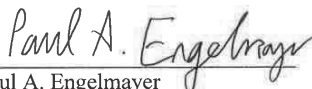
16 Cr. 5 (PAE)

ORDER

PAUL A. ENGELMAYER, District Judge:

The Court has received the parties' joint letter regarding next steps in this case. Dkt. 43. Consistent with the parties' joint recommendation, the Court hereby authorizes and directs the Receiver promptly to (1) delete any and all copies of data obtained from the Laptop in his possession (or that of his Retained Personnel), and (2) physically destroy the Laptop in a manner which renders the data stored thereon to be permanently and irrevocably inaccessible. Following the destruction of the Laptop, the Receiver is directed to send written notification to the Court of these actions. Pursuant to the parties' letter, the Court sets Mr. Knowles's sentencing for **Tuesday, December 6, 2016, at 11:30 a.m.**

SO ORDERED.

  
Paul A. Engelmayer  
United States District Judge

Dated: November 22, 2016  
New York, New York

## NOTES

The Use of Cloud Computing, Mobile Devices  
and Social Media in the Practice of Law  
(December 9, 2016)

Pamela A. Bresnahan

*Vorys, Sater, Seymour and Pease LLP*

Lucian T. Pera

*Adams and Reese LLP*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



New technologies have the potential to help lawyers practice smarter and more efficiently. However, such technology also contains risks for lawyers. Lawyers should be aware of those risks in order to avoid violating their ethical obligations. Lawyers should understand the implications that use of a particular technology will have on their obligations and utilize appropriate measures to comply with such obligations. This article addresses the implications of a lawyer's use of cloud computing, mobile devices and social media, as well as a lawyer's counseling of clients regarding their use of social media. The rules governing attorney conduct in the relevant jurisdiction should always be consulted when analyzing the use of these and other technologies.

## **I. OPERATING IN THE CLOUD AND MANAGING ETHICAL RISKS**

Technological advancements have led to the increased accessibility of information. In certain respects, information can be accessed from almost anywhere at any time, because of the prevalence of smartphones, other mobile devices and increased connectivity to the internet. Such advances provide increased opportunities for lawyers and law firms to access information related to their practices, while away from the office, through the use of "cloud computing." Cloud computing has been described as a "sophisticated form of remote electronic data storage on the internet. Unlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored 'in the cloud' is kept on large servers located elsewhere and maintained by a vendor."<sup>1</sup> Advantages that may be utilized from cloud computing include increased access to client data by a lawyer or law firm and increased access by clients to their own files over the internet.<sup>2</sup> Cloud computing can also help protect against loss of data by duplicating information on several servers and performing regular backups.<sup>3</sup>

However, lawyers and law firms that utilize cloud computing should be aware of certain ethical concerns that may arise from its use. The main concern is the confidentiality of the data being stored in the cloud. When operating in the cloud, client confidences and secrets are not under the

- 
1. Alabama State Bar, Ethics Op. 2010-02 (2010) (quoting Richard Acello, *Get Your Head in the Cloud*, ABA Journal, April 2010, at 28-29).
  2. *Id.*
  3. See Meghan C. Lewallen, Note, *Cloud Computing: A Lawyer's Ethical Duty to Act with Reasonable Care When Storing Client Confidences "In the Cloud,"* 60 Clev. St. L. Rev. 1133, 1139 (2013).

direct control of the lawyer or law firm and, thus, there is the potential for a third party to gain access to confidential client information.<sup>4</sup> Rule 1.6 of the ABA Model Rules of Professional Conduct provides that “[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [certain exceptions].”<sup>5</sup> If proper protocols are not put in place, a lawyer or law firm risks violating Rule 1.6 or its state analogs, when using the cloud to store confidential information.

Following reforms to the ABA Model Rules, a new subpart to Rule 1.6 reads “[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”<sup>6</sup> Revised comments [18] and [19] provide guidance regarding how to measure the reasonableness of efforts taken to prevent inadvertent disclosure or unauthorized access. Comment [18] states that:

[p]aragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer’s duties when sharing information with nonlawyers outside the lawyer’s own firm, see Rule 5.3, Comments [3]-[4].<sup>7</sup>

- 
4. Alabama State Bar, Ethics Op. 2010-02 (2010).
  5. ABA Model Rules of Prof’l Conduct R. 1.6(a) (2013).
  6. ABA Model Rules of Prof’l Conduct R. 1.6(c) (2013).
  7. ABA Model Rules of Prof’l Conduct R. 1.6, cmt. [18] (2013).

Comment [19] reads:

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.<sup>8</sup>

The language of these comments forms “the core set of principles used throughout virtually all ethics opinions in American jurisdictions that address confidentiality concerns in the cybersecurity context.”<sup>9</sup>

While there is the potential for unauthorized access to information a lawyer is required to keep confidential pursuant to Rule 1.6 or a state analog, ethics opinions addressing the use of cloud computing have nevertheless generally approved of the practice, subject to there being appropriate precautions put in place.<sup>10</sup> For example, the Nevada and Alabama State Bars have each issued ethics opinions calling for a standard of reasonable care. The Nevada State Bar has stated that an “attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney’s direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services” and “if the third party can be reasonably relied upon to maintain the confidentiality and agrees to do

---

8. ABA Model Rules of Professional Conduct R. 1.6, cmt. [19] (2013).

9. Peter Geraghty, Lucian T. Pera & Alfred J. Saikali, *Lawyer’s Obligations to Provide Data Security Arising from Ethics Rules and Other Law Specifically Governing Lawyers*, in *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals* 62, 63 (Jill D. Rhodes & Vincent I. Polley eds., 2013).

10. The ABA has compiled an extensive list of ethics opinions addressing the use of cloud computing. See ABA, *Cloud Ethics Opinions Around the U.S.*, available at [http://www.americanbar.org/groups/departments\\_offices/legal\\_technology\\_resources/resources/charts\\_fyis/cloud-ethics-chart.html](http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html).



so, then the transmission is permitted by the rules even without client consent.”<sup>11</sup> The Alabama Disciplinary Commission agreed, concluding that “a lawyer may use ‘cloud computing’ or third-party providers to store client data provided that the attorney exercises reasonable care in doing so.”<sup>12</sup> Such a duty requires that a lawyer be knowledgeable about how the data will be stored by the provider, about the security measures that will be put in place and to ensure that the provider will abide by a confidentiality agreement in its handling of data.<sup>13</sup> The Arizona State Bar has also weighed in, saying that lawyers “should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients’ documents and information.”<sup>14</sup> It is also important that a lawyer “know how data can be retrieved if the cloud computing provider goes out of business or if the cloud computing services are interrupted.”<sup>15</sup> The Iowa State Bar has also concluded that a lawyer “must ensure that there is unfettered access to the data when it is needed” and “must be able to determine the nature and degree of protection that will be afforded the data while residing elsewhere.”<sup>16</sup> With respect to selecting a provider, the Board of Professional Responsibility of the Supreme Court of Tennessee recently noted that the “primary obligation is to select a reliable provider under the circumstances. In making this selection, the lawyer should consider the provider’s ability to protect the information, to limit authorized access only to necessary personnel and to ensure that the information is backed up, is reasonably available to the lawyer and is reasonably safe from unauthorized intrusion.”<sup>17</sup>

Generally, exercising the proper level of care will require that the lawyer examine a cloud computing vendor’s terms of service to evaluate whether client information will be adequately protected.<sup>18</sup> If a lawyer is not competent to determine whether there are reasonable measures in place to protect client confidentiality through the use of a particular technology,

---

11. State Bar of Nevada, Standing Committee on Ethics and Professional Responsibility, Formal Op. No. 33 (2006).

12. Alabama State Bar, Ethics Op. 2010-02 (2010).

13. *Id.*

14. State Bar of Arizona, Ethics Op. 09-04 (2009).

15. Geraghty, Pera & Saikali, *supra* note 9, at 78 (citing Washington State Bar Ass’n, Op. No. 2215 (2012)).

16. Iowa State Bar Ass’n, Committee on Ethics and Practice Guidelines, Ethics Op. 11-01 (2011).

17. Bd. of Prof’l Responsibility of the Supreme Court of Tenn., Formal Ethics Op. 2015-F-159 (2015).

18. *See* Virginia State Bar, Legal Ethics Op. 1872 (2013).

“the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer.”<sup>19</sup> However, as commentators discussing Alaska Ethics Opinion 2014-3 have noted, “a lawyer’s decision to delegate to an IT professional the tasks relating to cloud computing is another form of outsourcing governed by [Alaska Rule of Professional Conduct 5.3].”<sup>20</sup> “Accordingly, the lawyer must make reasonable efforts to ensure that the IT professional’s conduct in overseeing these cloud computing issues is compatible with the lawyer’s professional obligations.”<sup>21</sup> Thus, delegation to an IT professional does not relieve a lawyer from his or her obligation to ensure that client confidentiality is adequately protected.

In 2013, the Maine Board of Overseers of the Bar provided a list of actions a lawyer should take with respect to the use of a cloud computing vendor, to be in accordance with the Maine Rules of Professional Conduct. The Board stated that a lawyer should ensure that a vendor: (1) explicitly agrees that it has no ownership or security interest in the data; (2) has an enforceable obligation to preserve security; (3) will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information; (4) has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing; (5) provides the firm with the right to audit the provider’s security procedures and to obtain copies of any security audits performed; (6) will host the firm’s data only within a specified geographic area; and, (7) provides the ability for the law firm, on demand, to get data from the vendor’s or third-party data hosting company’s servers for the firm’s own use or for in-house backup.<sup>22</sup>

The State Bar of California Standing Committee on Professional Responsibility and Conduct has also provided a list of factors an attorney should consider, prior to utilizing a new technology. Those factors include: (1) the attorney’s ability to assess the level of security afforded by the technology; (2) the legal ramifications of third-parties intercepting, accessing or exceeding authorized use; (3) the sensitivity of the particular information; (4) the impact to the client of an inadvertent disclosure; (5) the urgency of the situation; and, (6) client instructions and circumstances.<sup>23</sup>

---

19. Geraghty, Pera & Saikali, *supra* note 9, at 66.

20. Kevin Cuddy & John Cashion, *Ethics in the Cloud: When Is It Ok To Use Cloud Computing?*, 39 AK Bar Rag 16, 16 (2015).

21. *Id.*

22. Maine Board of Overseers of the Bar, Op. No. 207 (2013).

23. State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Op. 2010-179 (2010).

Even where a lawyer otherwise uses cloud computing in accordance with appropriate security measures, the Massachusetts Bar Association has opined that a lawyer “remains bound . . . to follow an express instruction from his or her client that the client’s confidential information not be stored or transmitted by means of the Internet, and all lawyers should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first obtaining the client’s express consent to do so.”<sup>24</sup> Therefore, a different storage method should be utilized for any client who objects to having his or her confidential information stored via the cloud. Additionally, a prudent lawyer should likely not rely exclusively on the cloud for storage of client information and should continue to maintain other storage systems as well, particularly when dealing with information that is extremely sensitive.

It is important that a lawyer be mindful of the standards set by their local jurisdiction, in connection with their use of cloud computing and protection of confidential information. Indeed, the increasing risk to client confidentiality posed by cloud computing has caused some to suggest that “it be mandatory for every lawyer to take a biennial CLE on recent metadata and cloud-computing advancements.”<sup>25</sup> Perhaps a harbinger of things to come, Florida recently became the first state to require continuing legal education in technology. On September 29, 2016, the Supreme Court of Florida adopted an amendment to the Rules Regulating the Florida Bar to require that three (3) out of thirty-three (33) hours of CLE over a three (3) year period be in an approved technology program.<sup>26</sup> While there is currently no such general technology CLE requirement outside of Florida, lawyers should nonetheless be vigilant that they understand and are in compliance with their relevant rules of professional conduct when utilizing cloud computing.

## II. USING MOBILE DEVICES

As with the use of cloud computing, a lawyer must guard against disclosure of confidential information and violations of other ethical duties through the

---

24. Mass. Bar Ass’n Ethics Op. 12-03 (2012).

25. Baylie Fry, *The Mandatory Continuing Legal Education Course on Metadata & Cloud-Computing: A Proactive Advancement to Avoiding Inadvertent Disclosures*, 7 Charlotte L. Rev. 27, 46 (2015).

26. See ABA/BNA Lawyer’s Manual on Prof’l Conduct, *Florida Is First State to Require Technology CLEs*, 32 Law. Man. Prof. Conduct 620 (2016).

use of mobile devices in his or her practice. Ethics opinions have provided guidance in this area as well.

The Florida Bar has concluded that “[i]f a lawyer chooses to use [sic] Devices that contain Storage Media, the lawyer has a duty to keep abreast of changes in technology to the extent that the lawyer can identify potential threats to maintaining confidentiality.”<sup>27</sup> In 2010, the Ethics 20/20 Commission’s Working Group on the Implications for New Technologies suggested certain precautions that a lawyer should take when utilizing portable devices. These precautions include:

1. Providing adequate physical protection or having methods for deleting data remotely in the event of a lost or stolen device;
2. Encouraging the use of strong passwords;
3. Purging data from a device before it is replaced with a new device;
4. Installing safeguards to combat viruses, malware and spyware;
5. Erecting firewalls;
6. Ensuring data is backed up frequently;
7. Updating operating systems to ensure the latest security protections are installed;
8. Configuring software and network settings to minimize risk;
9. Encrypting sensitive information;
10. Identifying and, when appropriate, eliminating metadata from electronic documents before sending them; and,
11. Avoiding public Wi-Fi hotspots when transmitting confidential information.<sup>28</sup>

In 2010, the State Bar of California Standing Committee on Professional Responsibility and Conduct examined a hypothetical fact pattern to determine if an attorney would violate the duties of confidentiality and competence by conducting legal research and e-mailing a client using a laptop connected to a public wireless internet connection at a coffee shop and from the attorney’s home, while connected to the attorney’s personal wireless system. The committee concluded that use of the public wireless system at the coffee shop risked violating both the duties of confidentiality

---

27. The Florida Bar Ethics Op. 10-2 (2010).

28. Geraghty, Pera & Saikali, *supra* note 9, at 72.

and competence because of the lack of security features provided in most public wireless systems, unless the attorney took appropriate precautions.<sup>29</sup> Such precautions might include “using a combination of file encryption, encryption of wireless transmissions and a personal firewall.”<sup>30</sup> However, if the situation involved a matter of particular sensitivity, an attorney “may need to avoid using the public wireless connection entirely or notify [the client] of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.”<sup>31</sup> On the other hand, the committee believed that an attorney’s use of a personal wireless connection at home would not constitute a violation of the duties of confidentiality and competence, so long as appropriate security features have been configured on the system.<sup>32</sup> This hypothetical fact pattern and analysis provides a good rule of thumb regarding the precautions that should be taken when utilizing mobile devices to conduct client business.

Lawyers must not only take appropriate precautions to protect confidential information, in light of their professional obligations, while using a mobile device, but also must take appropriate precautions when disposing of a device that has previously been used and that may contain confidential or other client information. When disposing of an electronic device, a lawyer “should ensure that confidential information has been removed.”<sup>33</sup> The failure to protect against disclosure of confidential information to a subsequent user of a device could result in a violation of Rule 1.6.<sup>34</sup> The Florida Bar has stated that, if a vendor is involved in the sanitization of a device upon disposal, it is not sufficient to merely obtain an agreement from the vendor that the device will be sanitized.<sup>35</sup> Rather, the lawyer has “an affirmative obligation to ascertain that the sanitization has been accomplished, whether by some type of meaningful confirmation, by having the sanitization occur at the lawyer’s office, or by other similar means.”<sup>36</sup>

---

29. State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Op. No. 2010-179 (2010).

30. *Id.*

31. *Id.*

32. *Id.*

33. Geraghty, Pera & Saikali, *supra* note 9, at 72 (citing Alabama State Bar, Ethics Op. 2010-02 (2010)).

34. Alabama State Bar, Ethics Op. 2010-02 (2010).

35. The Florida Bar, Ethics Op. 10-2 (2010).

36. *Id.*

### III. SOCIAL MEDIA

#### A. Lawyers Using Social Media

A lawyer utilizing social media should exercise due care to comply with his or her ethical and professional obligations. The nature of social media, and the ubiquity of its use in modern society, increases the potential for a lawyer to inadvertently violate a rule of professional conduct, should proper diligence not be exercised. A non-exhaustive list of potential pitfalls of a lawyer utilizing social media includes: (1) disclosure of confidential or privileged information; (2) communicating with represented parties; (3) inadvertent creation of attorney-client relationships; and, (4) violations of rules regarding legal advertising and/or solicitation of clients.<sup>37</sup> A resource that can help a lawyer deal with ethical concerns involving the use of social media is the Social Media Ethics Guidelines issued by the New York State Bar Association, which seeks to provide guidance on what is ethically permitted when using social media.<sup>38</sup> West Virginia also recently published a legal ethics opinion that discusses a variety of ethical issues surrounding the use of social media.<sup>39</sup>

Care must be exercised not to reveal any confidential or privileged information when posting to social media. For example, an attorney who published a public blog containing “confidential information about her clients and derogatory comments about judges”<sup>40</sup> received 60-day suspensions in both Illinois and Wisconsin as a result of such conduct.<sup>41</sup> A lawyer must also be extremely careful when deciding whether and how to respond to a negative review on social media, keeping in mind that the duty of confidentiality survives termination of an attorney-client relationship. For example, the Supreme Court of Georgia rejected an attorney’s petition for a mild form of voluntary discipline where the attorney had posted personal and confidential information about a

---

37. See Christina Vassiliou Harvey, Mac R. McCoy & Brook Sneath, *10 Tips for Avoiding Ethical Lapses When Using Social Media*, [http://www.americanbar.org/publications/blt/2014/01/03\\_harvey.html](http://www.americanbar.org/publications/blt/2014/01/03_harvey.html).

38. See N.Y. State Bar Ass’n, *Social Media Ethics Guidelines* (Jun. 9, 2015), available at <http://www.nysba.org/ComFedReports/>.

39. See West Virginia Legal Ethics Op. No. 2015-02 (2015).

40. *In re Peshek*, 798 N.W.2d 879, 879 (Wis. 2011) (per curiam).

41. See *id.*

former client in response to negative reviews that the client had posted on consumer websites.<sup>42</sup>

Bar Associations have also generally rejected the notion that the self-defense exception to Rule 1.6 is applicable in the context of a lawyer responding a negative review on social media.<sup>43</sup> In that regard, the Commercial and Federal Litigation Section of the New York State Bar Association issued a guideline that states that the prohibition against disclosure of confidential information “applies, even if the lawyer is attempting to respond to unflattering comments posted by the client.”<sup>44</sup> To aid lawyers who wish to respond to an unflattering post, the Pennsylvania Bar Association has proposed the following suggested response: “A lawyer’s duty to keep client confidences has few exceptions and in an abundance of caution I do not feel at liberty to respond in a point-by-point fashion in this forum. Suffice it to say that I do not believe that the post presents a fair and accurate picture of the events.”<sup>45</sup>

While lawyers must avoid revealing confidential or privileged information when posting information on social media, it may be permissible in certain jurisdictions for a lawyer to reveal information that has become a matter of public record. For example, the Supreme Court of Virginia held in 2013 that “[t]o the extent that the information is aired in a public forum, privacy considerations must yield to First Amendment protections. In that respect, a lawyer is no more prohibited than any other citizen from reporting what transpired in the courtroom.”<sup>46</sup> In *Hunter*, the Virginia State Bar instituted disciplinary proceedings against an attorney who authored a blog and argued that the attorney violated Rule 1.6 by revealing information “that could embarrass or likely be detrimental to his former clients by discussing their cases on his blog without their consent.”<sup>47</sup> However, the Supreme Court of Virginia agreed with the attorney’s contention that the Virginia State Bar’s interpretation of Rule 1.6 was unconstitutional because the matters discussed in the blog had already been revealed in public judicial proceedings and were protected by the First Amendment.<sup>48</sup> Therefore, the

---

42. *See In re Skinner*, 740 S.E.2d 171, 172 (Ga. 2013) (per curiam).

43. *See, e.g.* Penn. Bar. Ass’n, Formal Op. 2014-300 (2014).

44. N.Y. State Bar Ass’n, *Social Media Ethics Guidelines* (Jun. 9, 2015), available at <http://www.nysba.org/ComFedReports/>.

45. Penn. Bar Ass’n, Formal Op. 2014-200 (2014).

46. *Hunter v. Va. State Bar ex rel. Third Dist. Comm.*, 285 Va. 485, 503 (2013).

47. *Id.* at 492.

48. *Id.* at 502.

Court concluded that the state could not prohibit [through Rule 1.6] an attorney from discussing information about a client or former client that was not protected by the attorney-client privilege.<sup>49</sup> However, other jurisdictions may not allow the revelation of information relating to the representation of a client simply because the information at issue has already been made public. The Supreme Court of Colorado recently imposed a six month suspension on an attorney, with the requirement that the attorney petition for reinstatement, where the attorney had posted online responses to two negative reviews posted on Google+.<sup>50</sup> The attorney “revealed substantial information relating to the representations of . . . two clients, without authorization and without permission, in violation of Colo. RPC 1.6(a).”<sup>51</sup> The Presiding Disciplinary Judge determined it was “irrelevant . . . whether this information was already public: comment three to Colo. RPC 1.6(a) states that the rule ‘applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source.’”<sup>52</sup> Therefore, attorneys should be mindful of their local jurisdiction’s treatment of information that is a matter of public record before posting any such information on social media or elsewhere.

However, where Rule 1.6 or an appropriate analog is applicable, simply avoiding the explicit typing and posting of confidential information may not be enough in certain circumstances. Vigilance must be maintained to avoid inadvertent disclosures that may occur via social media, as a result of the use of certain technology or devices. For instance, geo-tagging a social media post or photograph may reveal the lawyer’s geographic location when travelling on confidential business, which could lead to a rule violation.<sup>53</sup>

Use of social media also creates the potential for a lawyer to communicate with a represented party, which is forbidden by ABA Model Rule 4.2 in circumstances where the represented person’s lawyer has not given consent to the communication.<sup>54</sup> The prior consent provision of state analogs of Rule 4.2, often referred to as the “no contact rule,” has been strictly interpreted. For example, the North Carolina State Bar and New York City Bar have each interpreted the rule to prohibit a

---

49. *Id.*

50. *People v. Isaac*, No. 15PDJ099, 2016 Colo. Discpl. LEXIS 109 (Colo. July 7, 2016).

51. *Id.* at \*8.

52. *Id.*

53. Harvey, McCoy & Sneath, *supra* note 37.

54. See ABA Model Rules of Prof’l Conduct R. 4.2 (2013).



lawyer from using the “reply all” feature when responding to an e-mail from an opposing attorney who has copied his or her client on the original e-mail, unless there is express or implied consent to do so based on the circumstances.<sup>55</sup> In the social media context, the sending of a Facebook friend request, LinkedIn invitation or other similar communication could be an improper communication when used in an attempt to gain access to a represented party’s private social media content.<sup>56</sup> However, a lawyer may generally view social media content that is not shielded by privacy settings and open to public viewing.<sup>57</sup> In addition to the caution lawyers should exercise in their communications on social media, the D.C. Bar recently urged lawyers to exercise caution when a social media site requests permission to access the lawyer’s e-mail contacts or to send e-mails to individuals in the lawyer’s address book.<sup>58</sup> Providing social media sites with such permissions “could potentially identify clients or divulge other information that a lawyer is obligated to protect from disclosure.”<sup>59</sup>

Attorney-client relationships may also inadvertently be created through use of social media if an attorney is not careful. Such relationships may be formed, in certain circumstances, when a lawyer responds to comments on a blog post or legal questions posted on a message board or similar communication.<sup>60</sup> Therefore, appropriate disclaimers should be utilized in connection with one’s social media activity, especially when responding to a prospective client’s request for information or advice.<sup>61</sup> Otherwise an attorney risks committing an ethical breach, or even legal malpractice, in a situation where the attorney is not consciously aware that he or she is even in an attorney-client relationship. However, one may generally write about legal topics in general, without creating an attorney-client relationship, so long as individual legal advice is not being communicated.<sup>62</sup>

---

55. See North Carolina State Bar, 2012 Formal Ethics Op. 7 (2013); The Ass’n of the Bar of the City of New York Committee on Professional and Judicial Ethics, Formal Op. 2009-1 (2009).

56. Harvey, McCoy & Sneath, *supra* note 37.

57. *Id.*

58. See D.C. Bar Ethics Op. 370 (2016).

59. *Id.*

60. Harvey, McCoy & Sneath, *supra* note 37.

61. *Id.*

62. Stephen C. Bennett, *Ethics of Social Networking*, 73 Albany L. Rev. 113, 123 (2009).

With respect to legal advertising via social media, a lawyer should be diligent to assure that any ads posted comply with the rules regarding attorney advertising in the appropriate jurisdiction.<sup>63</sup> The State Bar of California Standing Committee on Professional Responsibility and Conduct made clear in 2012 that material posted by an attorney on social media must comply with the rules governing attorney advertising in the state, so long as the material posted satisfies the criteria used to constitute a “communication” within the meaning of the rules.<sup>64</sup> Therefore, attorneys must be mindful of the local rules governing advertising before posting messages. For example, use of “puffery” and false statements of material fact or law should be avoided.<sup>65</sup> Additionally, some states prohibit the use of words such as “specialist,” “certified” or “expert” without possessing appropriate qualifications.<sup>66</sup> Particular attention must be paid to social networking sites that invite lawyers to identify “specialties” or areas of expertise in their profiles, such as Avvo and LinkedIn.<sup>67</sup> Otherwise, an attorney risks committing an inadvertent violation of the rules governing attorney advertising.

Attorneys should be mindful of these and other rules of professional conduct that may be implicated through their use of social media. Therefore, it is recommended that attorneys consult their local rules of professional conduct and ethics opinions and judicial opinions interpreting those rules, prior to engaging in the use of social media.

## **B. Lawyers Advising Clients About Their Use of Social Media**

In certain scenarios, information and photographs posted on social media can have a great effect upon a client’s case. Therefore, lawyers should be aware of the ethical implications of providing advice regarding their clients’ social media use. Important to consider is whether a lawyer may advise a client about what to post or not post on social media and whether the lawyer may advise a client to remove an existing post from a social media account.

---

63. Michael E. Lackey, Jr. & Joseph P. Minta, *Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging*, 28 Touro L. Rev. 149, 158 (2012).

64. See The State Bar of California, Standing Committee on Professional and Responsibility and Conduct, Formal Op. No. 2012-186 (2012).

65. *Id.* at 159; see also ABA Model Rules of Prof’l Conduct R. 4.1 (2013).

66. See, e.g., Ill. Rules of Prof’l Conduct R. 7.4(c); N.Y. Rules of Prof’l Conduct R. 7.4(a).

67. Harvey, McCoy & Sneath, *supra* note 37.

In certain cases, competent representation includes providing advice to a client regarding the legal ramifications of social media postings, including existing and future postings, if the postings could be relevant to the legal matter.<sup>68</sup> Put another way, “an attorney may properly review a client’s social media pages, and advise the client that certain materials posted on a social media page may be used against the client for impeachment or similar purposes.”<sup>69</sup> Both the Florida Bar and New York County Lawyers Associations have also concluded that a lawyer may ethically advise a client to use the highest level of privacy settings on the client’s social media accounts.<sup>70</sup> Use of such settings will typically prevent adverse counsel from obtaining direct access to the social media page without requesting access through formal discovery.<sup>71</sup>

Ethics opinions addressing whether a lawyer may counsel a client to remove an existing social media post that may be at issue in a legal matter point to the law of spoliation of evidence as the relevant inquiry. A lawyer may not counsel a client to engage in conduct that the lawyer knows is criminal or fraudulent or to unlawfully obstruct another party’s access to evidence.<sup>72</sup> Therefore, a lawyer should not advise a client to remove an existing social media post, if doing so would constitute spoliation of evidence in the relevant jurisdiction.<sup>73</sup> Additionally, a lawyer may not advise a client to post information on social media that is false or misleading.<sup>74</sup> However, according to the Florida Bar, if there would be no violation of the rules governing spoliation or preservation of evidence, a lawyer may advise a client to “remove information relevant to the foreseeable proceeding from social media as long as the social media information or data is preserved.”<sup>75</sup> Thus, a lawyer should be aware that, even when permissibly counseling a client to remove certain information from social media, he or she must also “take appropriate action to preserve the information in the event it should prove to be relevant and discoverable.”<sup>76</sup>

---

68. North Carolina State Bar, 2014 Formal Ethics Op. 5 (2015).

69. N.Y. Cnty. Lawyers Ass’n Ethics Op. 745 (2013).

70. *Id.*; The Florida Bar Ethics Op. 14-1 (2015).

71. N.Y. Cnty. Lawyers Ass’n Ethics Op. 745 (2013).

72. *See* ABA Model Rules of Prof’l Conduct R. 1.2(d), 3.4(a) (2013).

73. North Carolina State Bar, 2014 Formal Ethics Op. 5 (2015).

74. Pennsylvania Bar Ass’n Formal Op. 2014-300 (2014).

75. The Florida Bar Ethics Op. 14-1 (2015).

76. The Philadelphia Bar Ass’n Prof’l Guidance Committee Op. 2014-5 (2014).

#### **IV. CONCLUSION**

Modern technology, in many respects, has changed the manner in which attorneys practice law. New technologies allow for increased access to information and increased efficiency. However, use of technologies such as cloud computing, mobile devices and social media contain inherent risks, especially with regard to the duties one has to protect their clients' confidential information. Therefore, it is important for attorneys to understand the ethical concerns that must be addressed through their use of such technologies (and future technologies) in connection with the practice of law. Proper care and precautions should always be utilized to ensure compliance with one's appropriate ethical and legal concerns and the relevant rules governing attorney conduct should be reviewed prior to one's use of a new technology. Below are fifteen hypothetical scenarios that demonstrate some of the ethical concerns addressed above.

## **Hypothetical 1 – Calming Nelly**

You have a partner who can a bit of a “nervous Nelly.”

He worries about nearly everything and, because you have a late-model iPhone and an iPad, he frequently asks you what sometimes seem to be frivolous questions. He must have just read some marketing piece from an electronic security firm, because he comes into your office in a panic with several questions.

*May a lawyer ethically communicate with a client using...*

*A cordless home phone?*

*A cell phone?*

*Texting on a cell phone?*

*Exchanging Facebook messages?*

*Unencrypted email?*

*Gmail or other online email services?*

## **Hypothetical 2 – Clouds on the Horizon**

When your partner tells you it’s time to replace the network server where your office keeps email and documents, she also tells you that the law firm down the hall just replaced their server and stores all their information “in the cloud.” And, she says, they say they have saved a *lot* of money doing so.

*May you store confidential client communications in the “cloud”?*

## **Hypothetical 3 – The Good Son**

You represent an elderly couple in a lawsuit.

You regularly communicate with them by email, sending them copies of correspondence with opposing counsel, pleadings, and the like.

A few months into your representation you learn that they routinely ask their son to help them by printing off your emails to them.

*Is there any advice you should give the couple about this?*

## **Hypothetical 4 – Advising the Restless Employee**

You represent a licensed securities broker employed by a big brokerage. She is considering her options for staying with the firm or moving to another firm and wants your advice on her legal rights and obligations.

Shortly after your first meeting, in your law office, she emails you from her company email address.

*Is there any advice you should give the broker about this?*

### **Hypothetical 5 – Reply to All**

You have been representing a company for about 18 months in an effort to negotiate the purchase of a patent from a wealthy individual inventor.

The negotiations have been very cordial at times, but occasionally turn fairly contentious. You and your company's vice president have met several times with the inventor and his lawyer, both at the inventor's home and in a conference room in your client company's headquarters. After some of the fruitful meetings, you and the other lawyer have exchanged draft purchase agreements, with both of you copying your clients – the vice president and the inventor.

Last week things turned less friendly, and you heard that the inventor's lawyer might be standing in the way of finalizing a purchase agreement. This morning you received a fairly chilly email from that lawyer, rejecting your latest draft purchase agreement and essentially threatening to "start all over again" in the negotiations given what he says are your client's unreasonable demands. As in earlier emails, the other lawyer copied the email to his client, the inventor.

*May you respond to the other lawyer's email using the "Reply to All" function, and defending your client's positions in the negotiations?*

### **Hypothetical 6 – Stolen Laptop**

Late one evening, you get a frantic phone call from your associate.

She says she stopped off for dinner with her husband on the way home from work and that, on leaving the restaurant, she found her car window smashed and her briefcase stolen. And her firm-issued laptop that had been inside was gone, too.

*What do you do?*

### **Hypothetical 7 – The Departed**

A little more than two weeks ago, the bright young associate you raised from a pup gave her two-week notice. Her last day was last Tuesday. Her departure was reasonably cordial.

This morning, your office manager tells you there's a problem.

The departed associate had a personal laptop and smartphone she used for work. They were configured, with your office's help, to access her office email and other office systems remotely. And she never got

around to honoring the office manager's request to bring the laptop and phone in so that your tech guy could remove firm email and other files from them. Your office manager says her access to email firm systems is cut off, but he's convinced that the departed associate still has firm data on her devices.

*Do you have an ethics problem?*

### **Hypothetical 8 – Road Warrior**

One of the lawyers in your office lives on the road.

For that reason, she also lives on her laptop.

When you have traveled with her, you have noticed that she always tries to find a place in a courthouse, coffee shop, hotel lobby, hotel room, or airport that has free wi-fi, to do her work. Occasionally, she even pays a few bucks for a wi-fi connection.

*Is the firm's and its clients' information safe in her hands?*

### **Hypothetical 9 – Cheapo Neighbors**

About six months ago, your paralegal convinced you to buy and install a wi-fi hotspot in your office, saying it was cheap, and would let you and others in your office connect to firm systems with your tablets and laptops without using internet cables. And, your paralegal said, clients could use it in the lobby while they waited for appointments.

Suddenly, within the last few weeks, you can never log on to the wi-fi. After investigating, your office manager tells you he thinks may be folks outside the office are using it and hogging capacity. After all, he says, there's no password on the wi-fi and the signal can be reached by the lawyers to whom you lease the second floor and customers in the Subway sandwich shop across the driveway.

*Do you have a problem?*

### **Hypothetical 10 - Handshake**

You are the firm's managing partner.

After interviewing three separate technology companies, you settle on one to replace your former consultant, whose prices just got too high.

As you are concluding your call to the company you decided to hire, you casually mention to the owner, "Well, send me over your standard contract, with the terms and prices we discussed, and we'll look it over." The company owner is quiet for a moment and says, "Well,

we have usually just done business on a handshake. Is that OK? We certainly trust you.”

*Do you need a written agreement? If so, what should it say?*

### **Hypothetical 11 – What, Me Worry?**

One day, as you are having lunch with two other lawyers from your office, one brings up a report he read about a big law firm whose computers were hacked. Then one of the lawyers says, “Well, thank goodness we don’t have any of those big international clients. Who’d want to hack us?”

*What should you do to protect your office?*

### **Hypothetical 12 – Going Paper-Less**

Last month, you hired a new paralegal, replacing your former long-time paralegal.

One morning, your new paralegal suggests that you really could be using your office’s case management software much more fully – for example, storing all documents and email about a matter there, and going paperless. “In fact,” she said, “at my old firm, we got rid of almost everything in our paper client files, kept it all nicely organized in the same program you have, and turned the file room into an office for another lawyer. Just give me the go-ahead and I’ll make it happen.”

*May you ethically do away with paper client files and go “paperless”?*

### **Hypothetical 13 – File Storage Company**

Six months ago, you successfully closed a client’s acquisition of a piece of real property. All your post-deal clean-up work is done, all funds disbursed, and all fees and expenses paid.

You write the client a letter thanking her for calling on you, telling her the matter is over, and telling her that you’d be happy to provide her a copy of her client file if she would like, but that your normal document retention policy is to keep files for two years and then destroy them, and that this is your plan as to her file. The client never responds.

*Are you required to keep the file? If so, for how long?*



## **Hypothetical 14 – File Converter**

Same facts as Hypothetical 13, but...

The client responds to your letter by asking for a copy of the file in electronic format, with everything in PDF files.

As you review your file materials, you see that there are some paper documents in the file, some handwritten notes, some drafts with handwritten markups by you and people in your office, email in Microsoft Outlook, a bunch of Word documents, and a few Excel spreadsheets.

*Are you required to honor the client's request?*

## **Hypothetical 15 – Old Laptops**

For several years, you have served on the board of a non-profit organization that helps disadvantaged high school students learn about the business world.

At a quarterly board meeting, you hear some discussion about the difficulty the group is having raising funds to buy more laptops for the students to use in their internships with local businesses.

Suddenly, you remember that, over the next few months, your office is upgrading its laptops and will have about five old ones it no longer needs. You mention this, and the organization's staff director gets very excited, saying they might well be able to clean them up, do some inexpensive upgrades, and let the students use them.

*May you donate your old laptops to the organization?*

## NOTES

## NOTES

Summary of 2016 Internet of Things Cases  
(January 2017)

James G. Snell  
Christian Lee  
*Perkins Coie LLP*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



## BIOGRAPHICAL INFORMATION

Jim Snell is a Privacy and Security and Intellectual Property Litigation Partner in Perkins Coie's Palo Alto office and can be reached at [jsnell@perkinscoie.com](mailto:jsnell@perkinscoie.com) and 650-838-4367. Christian Lee is a Privacy and Security and Intellectual Property Litigation Associate in Perkins Coie's Palo Alto office and can be reached at [clee@perkinscoie.com](mailto:clee@perkinscoie.com) and 650-838-4408.



## A. INTRODUCTION

The following is a summary of some of the more interesting Internet of Things litigation matters, including a range of technology areas such as smartphone apps, automobiles, medical devices, and consumer electronics.

## B. CASES

### 1. Smartphone Applications

#### a. ***Satchell v. Sonic Notify, Inc. et al.*, 4:16-cv-04961-JSW (N.D. Cal. Aug. 29, 2016)**

This case alleges that the Golden State Warriors basketball team partnered with an app developer to offer an app that contained “beacon” functionality used at Warriors games. The “beacon” technology determined the location of a smartphone by measuring the distance between the phone and nearby towers. (Each tower emitted a unique signal). As an app user walked by, his phone would detect the beacon’s signal and determine its location by the unique beacon signal. Ads, promotions, and other interactive functions were then triggered based on the user’s location.

The beacon signals in this case used unique audio data that was particular to each tower. The audio was picked up by a smartphone’s microphone, which triggered the beacon functionality.

Plaintiff alleged that the app turns on a user’s microphone and kept it on, continually listening in on and recording any audio within range of the microphone. Plaintiff claimed that she was injured as a result of the unauthorized recording of her oral communications which allegedly led to wear and tear on her smartphone and diminished her use, enjoyment, and utility of her phone.

Plaintiff claimed that the app’s purported recording functionality constituted a violation of the federal Electronic Communications Privacy Act, which prohibits a person from intercepting any oral communication or from using the content of any oral communication that was obtained from an interception.

Defendants moved to dismiss, arguing, first, that the beacon audio signals were on a frequency that was inaudible to the human ear, and that the app was programmed to detect only these frequencies. Accordingly, this meant that the app did not record any person’s “oral communications.” Second, Defendants noted that “interception” under the Wiretap Act means the “acquisition” of the contents of



an oral communication, which Defendants did not do because any data that was recorded by the app was kept on the phone and not transmitted to the Defendants.

Finally, Defendants also moved to dismiss based on plaintiff's lack of Article III standing under *Spokeo* because Plaintiff did not actually suffer any injury due to the alleged interception of communications, and because the recording did not cause wear and tear to Plaintiff's smartphone.

As of the date this article was submitted, the motion to dismiss remains pending.

**b. *FTC v. Aura Labs, Inc.*, 8:16-CV-2147 (C.D. Cal. Dec. 2, 2016)**

This FTC enforcement action ended in settlement. Aura Labs is an app developer that marketed the Instant Blood Pressure app, which uses mathematical algorithms, mobile device measurements, and consumer-inputted data (gender, age, height, weight) to purportedly measure blood pressure. The app instructed users to remove their outer clothing, place their index finger over a smartphone camera's lens, and place the phone against the left side of their chest, after which the app would purported display systolic and diastolic blood pressure measurements. The app purportedly had revenues of over \$600,000 from approximately one year of sales.

The FTC alleged that the app claimed that it measured blood pressure as accurately as machines relying on traditional blood pressure cuffs, and that it was a cuff replacement. Additionally, the FTC contended that Aura's CEO and President left a five star review for the app, calling it a "breakthrough" in the industry, among other things.

The FTC filed suit, claiming that Aura Labs violated Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, based on Aura Labs' misrepresentation of the app's ability to (1) serve as a replacement for the traditional blood pressure cuff; and (2) measure blood pressure as accurately as traditional blood pressure cuffs. The FTC also faulted Aura Labs for the allegedly deceptive use of its CEO's endorsement of the app, and for the company's failure to disclose that some of the app's endorsements were made by Aura Labs' employees.

Aura Labs settled with the FTC, agreeing to cease certain representations about the comparative efficacy of the app's ability to measure blood pressure and about the health benefits of the app,

unless it could support its claims with reliable scientific evidence. Aura Labs also agreed to cease its use of certain endorsements.

## **2. Automobiles**

### **a. *Cahen v. Toyota Motor Corp., et al.*, 3:15-cv-01104 (N.D. Cal. March 10, 2015)**

This case was brought against three Defendant automobile manufacturers whose vehicles used electronic control units (“ECUs”), which are small computers that control various vehicle operations. ECUs allegedly communicated among each other through controller area network packets (“CAN packets”), which Plaintiffs contended were not encrypted or authenticated, and exposed to hacking. As a result, Plaintiff’s contended, anyone with physical access to the vehicle could interfere with the CAN packets or send malicious CAN Packets to the ECUs. Additionally, the vehicles had wireless Bluetooth capabilities that were also allegedly susceptible to hacking.

Importantly, none of the plaintiffs alleged that they were actually hacked. They merely pleaded that hacking was an “imminent eventuality” based on journal articles and research studies, which showed hacking in controlled situations.

Plaintiffs also alleged that the Defendants collected data about its drivers, including geographic location, driving history, and vehicle performance, and then shared that data with third parties without securing the transmission.

Plaintiffs brought multiple claims, depending on each plaintiff’s residency. For the California plaintiffs, claims included violation of California’s Unfair Competition Law; violation of California’s Consumer Legal Remedies Act; violation of California’s False Advertising Law; breach of implied warranty of merchantability; breach of contract; fraudulent concealment; violation of California’s Song-Beverly Consumer Warranty Act; and invasion of privacy.

The Defendants moved to dismiss based on the failure to establish Article III standing, failure to state a claim, and preemption by federal law. The court granted the motion to dismiss in its entirety. On Article III standing, the court pointed out that plaintiffs did not allege that any hacking incidents, outside of the controlled settings, actually occurred. Thus, there was no injury to confer standing on plaintiffs other than a speculative allegation that someday someone could hack plaintiffs’ vehicles.

Plaintiffs also attempted to establish Article III standing based on the purported economic loss that flows from the risk of further injury. The court also held that the alleged economic loss flowing from the *risk* of future hacking was not a cognizable injury because the alleged economic injury rested solely on the speculative risk of future hacking.

On March 22, 2016, plaintiffs filed an appeal to the 9th Circuit, arguing primarily that there is Article III standing based on (1) allegations that a plaintiff overpaid - or would not have paid for - a vehicle had they known about the alleged defect; and (2) invasion of privacy under the California Constitution.

As of the date this article was submitted, the appeal remains pending.

***b. Flynn v. FCA US LLC, No. 3:15-cv-855 (S.D. Ill. Aug. 4, 2015)***

This case is similar to *Cahen* and involves owners of Chrysler vehicles who alleged design flaws in the vehicle computer systems, and sued Chrysler and Harmon International, the manufacturer of the uConnect computer system. In 2015, WIRED magazine published an article that claimed to demonstrate, under controlled testing, that the uConnect system could allow hackers to take control of various functions of the vehicle, including dashboard functions, transmission, steering, and braking. The hacking was done via a laptop 10 miles away from the vehicle.

After the article was published, Chrysler recalled 1.4 million vehicles for a software update. Chrysler also issued a press release, pointing out that the hacking technique was very difficult, that no defect has been found, and that the recall was being conducted only out of an abundance of caution.

Plaintiffs filed suit and asserted various state laws, including violation of the Magnuson-Moss Act and implied warranty of merchantability, for defendants allegedly putting vehicles into circulation with design flaws; fraud and consumer protection statutes based on lying or failure to disclose vulnerabilities; negligence; and unjust enrichment.

Plaintiffs also alleged as damages overpayment for vehicles that were initially defective, that continuing vulnerabilities had diminished the market value of the vehicles, and an alleged increased risk of injury or death caused by the vulnerabilities.

The Defendants moved to dismiss, primarily on the basis of the lack of Article III standing contending that alleged risks of future injury and fear of that injury do not create standing unless there is a substantial risk that the feared injury will be realized.

On September 23, 2016, the court partially granted the motion to dismiss, holding that the risk of future injury, and the fear of those future injuries, did not confer Article III standing. The court highlighted the attenuated chain of events that would need to occur for a serious injury to befall the plaintiffs: the vehicle would need to be hacked by one sophisticated enough to remotely access the vehicle; the hack would need to occur despite the software updates; the hack would need to involve the vehicle's critical systems; and the hack would need to cause a wreck of the magnitude to cause serious injury or harm.

However, unlike *Cahen*, the court was persuaded that there was alleged injury in that plaintiffs claimed to have overpaid for the vehicles, and that the vehicle defects lowered their market value. The defendants argued that the overpayment or diminution of value was speculative because no consumer had actually been injured or killed due to the alleged defect, but the court overruled these arguments, holding that there were alleged defects in the vehicle other than safety-related defects, which supported standing. The court also noted that numerous consumers reported during the recall that their vehicles were remotely unlocked and robbed by hackers, which supported injury-in-fact. The court thus refused to dismiss these claims and, as of the date this article was submitted, the case remains pending.

### **3. Medical Devices**

#### **a. *Clinton W Ross Jr v. St. Jude Medical, Inc. et al.*, 2:16-cv-06465-DMG-E (C.D. Cal. Aug. 26, 2016)**

Plaintiff's filed a lawsuit against St. Jude Medical, a hospital, and Pacesetter, Inc., the manufacturer of pacemakers. Plaintiffs allege that when a pacemaker is implanted, the physician uses a "device programmer" to adjust the settings on the pacemaker. The device programmer typically communicates with the pacemaker via a telemetry wand, which is placed outside of the body and over the pacemaker to obtain readings and make adjustments. Telemetry wands can be placed in a patient's home, allowing for readings without going to the doctor's office.

Certain models of pacemakers utilized radiofrequency (RF) wireless technology, which Plaintiff claimed allowed detection and was vulnerable to unauthorized access, and which in turn could result in privacy breaches. Plaintiffs alleged that a St. Jude brochure claimed that patients' data would be uploaded to its "safe and secure web-based data management system that is protected with industry-standard safety protocols." Plaintiff also contended that St. Jude claimed that its system was the first medical device network to be awarded the "ISO 27001 certification, a stringent worldwide information security standard."

An equity research firm issued a report contending that the pacemakers with RF capabilities had vulnerabilities, including the lack of security defenses such as "strong" authentication, encrypted software, and anti-tampering mechanisms. These security measures, Plaintiff contended, were present in technology used by other pacemakers. The report also noted that the lack of defenses allowed the research company to demonstrate (1) a "crash attack" that would cause the pacemaker to pace at a rapid rate; and (2) drain the pacemaker's battery down to a useful life of two weeks.

Plaintiff did not himself experience any of these attacks, but claimed that as a result of learning about these security issues, he ceased using the telemetry device at home (but did not cease using his pacemaker).

Plaintiff claimed breach of express warranty, based on St. Jude's alleged claims about the benefits of the pacemaker and home-monitoring capabilities, and the security of monitored health data; fraudulent concealment, based on St. Jude's purported knowledge that the pacemakers and home telemetry device lacked the necessary security yet failed to disclose this to consumers; negligence; and unjust enrichment.

Plaintiff here voluntarily dismissed the case, without prejudice, before Defendants responded to the complaint.

#### **4. Consumer Electronics**

**a. *In re Vizio, Inc., Consumer Privacy Litigation*, 8:16-md-02693-JLS-KES (MDL) (C.D. Cal. Apr. 11, 2016)**

This is a multidistrict litigation involving Vizio, a manufacturer of smart TVs. The TVs contained content recognition and tracking software, along with integrated Internet capabilities, that allegedly tracked what viewers were watching in real-time. The

software, according to plaintiffs, tracked anything viewed on the TV, including content from cable/satellite providers, streaming devices, and gaming consoles. The data was then sent to Vizio and/or advertisers. The software also scanned devices located on a viewer's network which is normally blocked by network firewalls, but the software was able to do so because it was executed from a TV that was already connected to the user's network.

The software was opt-out instead of opt-in, and this recognition and tracking functionality was called "Smart Interactivity" that "[e]nables program offer and suggestions" allegedly with no further description.

Plaintiffs pled a variety of state unfair business practice claims (such as the California Consumers Legal Remedies Act; Unfair Competition Law; False Advertising law, fraudulent omission, and negligent omission, based on the failure to disclose the tracking software; and unjust enrichment), violation of the Wiretap Act, and violations of state and federal laws governing video rental and sales privacy.

Vizio moved to dismiss, primarily on the grounds that even if there were statutory violations, there was a lack of Article III standing because there was no injury in fact. Vizio highlighted that courts post-*Spokeo* have continued to hold that merely disclosing information in violation of a statute did not establish concrete injury.

As of the date this article was submitted, the motion to dismiss remains pending.

**b. *In re: VTech Data Breach Litigation, No. 1:15-CV-10889 (N.D. Ill. Dec. 3, 2015)***

VTech Electronics is a manufacturer and distributor of digital learning toys for preschool and grade school aged children. The toys included tables, smartwatches, and handheld touch learning devices. VTech's toys depended on an online app store called the "Learning Lodge" where users download educational content, and one functionality, called "Kid Connect," allows parents (using regular cell phones) to contact children (using VTech devices). VTech required users to register with VTech before allowing them to access software and hardware updates. Mandatory registration information included name, home addresses, email addresses, and passwords. A child was also allowed to create a profile, including name, date of birth, gender, and photographs. If a child created a profile, then it was linked to the registration information, which included a

home address. Some of VTech's toys contained a camera, which allowed children to take pictures and upload them online. Some toys also allowed children to transmit voice messages through VTech servers.

In November 2015, a hacker infiltrated VTech's computer systems to download personally identifiable information (PII) of more than 10 million individuals using VTech's services, including children. The names, photographs, birthdates, and physical addresses of children were among the PII taken in the data breach. This data breach was alleged to be the largest that involved minors. VTech subsequently disabled the KidConnect service, and disabled certain Learning Lodge functionality.

VTech's terms and conditions, according to plaintiffs, contained statements by VTech about security of data, noting that the company would "protect privacy and personal information" and take "reasonable precautions to keep personal information secure."

Plaintiffs did not allege that any of the hacked PII was disseminated by the hacker.

Plaintiffs alleged that users reasonably expected industry-standard data security, but that VTech failed to deliver this, which allowed a hacker to access children's PII. Plaintiffs also alleged that they paid substantially more for VTech's products than they would have had they known that VTech's security was sub-standard. Finally, Plaintiffs alleged that the data breach caused potential risks of future harm.

Plaintiffs claimed breach of contract, based on VTech allegedly overpromising on the security and actual functionality of its products than it delivered; breach of implied covenant of good faith and fair dealing, based on the same contract; breach of implied warranty of merchantability, based on the defective devices; violation of Illinois consumer protection act, based on allegedly unreasonable security practices and other predicate statutory violations; and declaratory judgement.

VTech moved to dismiss based on lack of standing since Plaintiffs only pled the potential risk of future harm and not actual harm. VTech also moved to dismiss Plaintiffs claim that the products had diminished value because Plaintiffs did not plead that they purchased the products because of the online functionality or that products without online functionality were available at different pricing.

As of the date this article was submitted, the motion to dismiss remains pending.

**c. *N.P. v. Standard Innovation (US), Corp., 1:16-CV-08655 (N.D. Ill. Sept. 2, 2016)***

Plaintiffs brought this lawsuit against Standard Innovation (“SI”), which allegedly sells an adult personal stimulation device with an associated app, which allowed the user to remotely control the devices settings and features.

Plaintiff alleged that SI collected data regarding consumers’ use of the devices, including the date and time of each use and the devices settings, without providing notice of its collection and use. This information was allegedly transmitted to SI’s servers. Plaintiff claimed that she would not have purchased SI’s device had she known about Defendant’s monitoring, collection, and transmission of her personal data.

Plaintiff claimed that SI’s conduct violated the Wiretap app, the Illinois Eavesdropping Act, the state deceptive trade practices act, and alleged publicity and contract torts.

Before SI filed an answer, the parties participated in mediation with JAMS and reached a settlement, the terms of which are unknown.

**d. *Cheatham v. ADT Corporation and ADT LLC, 2:15-CV-02137-DGC, (D. Ariz. Oct. 23, 2015)***

ADT is a company that offers wireless home security equipment and monitoring services. According to plaintiffs, some of the packages it sold contained manuals warning that the system’s wireless signals could be interfered with, while others did not.

In 2014, a security researcher made a presentation that highlighted the alleged susceptibility of ADT’s system to hacking: the research claimed he could jam the security systems to disable the wireless sensors (but not the cameras), hack into the system to view the sensor and video feeds, or set off the alarms of the security system. These hacks required a software-defined radio (“SDR”), combined with a special computer program.

Plaintiff filed suit against ADT after the researchers findings were made public. Plaintiff asserted various claims, based on allegations that ADT overpromised on its security measures and did



not adequately disclose the system's vulnerabilities. Other plaintiffs in different states similarly filed suit.

In December 2016, Plaintiff filed a motion to certify a class, and on January 10, 2017, ADT opposed, contending that Plaintiff did not have Article III standing under *Spokeo* because the system she purchased came with a manual that expressly warned of the risk of "deliberate jamming." This meant that Plaintiff's alleged injuries could not be traced back to ADT, a requirement of Article III injury.

Additionally, ADT opposed class certification by arguing that what the proposed class members knew about the vulnerability of their systems varied greatly, such that there was insufficient commonality among them.

The motion remained pending as of the date this article was submitted.

## **5. World-Wide Web Outage**

In October 2016, much of the United States was impacted by a massive and sustained denial of service (DOS) attack that blocked users from accessing some of the Internet's top destinations, including Amazon, Netflix, Reddit, Spotify, Tumblr, and Twitter. The malware underlying for the attack is called Mirai, which was reportedly released on the dark web in September 2016.

Mirai reportedly operated by scouring the Internet for unsecure IoT devices and turning them into a bot web for DoS attacks on a massive scale. Mirai looked for devices that had factory-default usernames and passwords, and co-opted them for use. One analysis found 68 username/password pairs that were tested against devices; if they matched, Mirai gained access to the device and co-opted it into the attack.

Many IoT devices essentially have two sets of username/password access: one to access a web-based administrative panel in software that ships with the products; and another set of username/password for access to the firmware itself and which is hardcoded and cannot practically be changed. The latter type of access depends on command-line interfaces, such as Telnet and SSH, with no graphical user interface for the typical user to change it. In October 2016, more than 500,000 of these vulnerable systems reportedly existed, all of which were thus susceptible to joining the Mirai attack.

## NOTES

## NOTES

President's Council of Advisors on Science  
and Technology, Report to the President—  
Big Data and Privacy: A Technological  
Perspective (May 2014)

Submitted by:  
Christin S. McMeley  
*Davis Wright Tremaine LLP*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.





REPORT TO THE PRESIDENT  
BIG DATA AND PRIVACY:  
A TECHNOLOGICAL  
PERSPECTIVE

Executive Office of the President  
President's Council of Advisors on  
Science and Technology

May 2014







REPORT TO THE PRESIDENT  
BIG DATA AND PRIVACY:  
A TECHNOLOGICAL PERSPECTIVE

Executive Office of the President  
President's Council of Advisors on  
Science and Technology

May 2014







## **About the President's Council of Advisors on Science and Technology**

The President's Council of Advisors on Science and Technology (PCAST) is an advisory group of the Nation's leading scientists and engineers, appointed by the President to augment the science and technology advice available to him from inside the White House and from cabinet departments and other Federal agencies. PCAST is consulted about, and often makes policy recommendations concerning, the full range of issues where understandings from the domains of science, technology, and innovation bear potentially on the policy choices before the President.

For more information about PCAST, see [www.whitehouse.gov/ostp/pcast](http://www.whitehouse.gov/ostp/pcast)





## The President's Council of Advisors on Science and Technology

### Co-Chairs

**John P. Holdren**

Assistant to the President for  
Science and Technology  
Director, Office of Science and Technology  
Policy

**Eric S. Lander**

President  
Broad Institute of Harvard and MIT

### Vice Chairs

**William Press**

Raymer Professor in Computer Science and  
Integrative Biology  
University of Texas at Austin

**Maxine Savitz**

Vice President  
National Academy of Engineering

### Members

**Rosina Bierbaum**

Dean, School of Natural Resources and  
Environment  
University of Michigan

**S. James Gates, Jr.**

John S. Toll Professor of Physics  
Director, Center for String and Particle  
Theory  
University of Maryland, College Park

**Christine Cassel**

President and CEO  
National Quality Forum

**Mark Gorenberg**

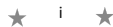
Managing Member  
Zetta Venture Partners

**Christopher Chyba**

Professor, Astrophysical Sciences and  
International Affairs  
Director, Program on Science and Global  
Security  
Princeton University

**Susan L. Graham**

Pehong Chen Distinguished Professor  
Emerita in Electrical Engineering and  
Computer Science  
University of California, Berkeley



**Shirley Ann Jackson**

President  
Rensselaer Polytechnic Institute

**Richard C. Levin** (*through mid-April 2014*)

President Emeritus  
Frederick William Beinecke Professor of  
Economics  
Yale University

**Michael McQuade**

Senior Vice President for Science and  
Technology  
United Technologies Corporation

**Chad Mirkin**

George B. Rathmann Professor of Chemistry  
Director, International Institute for  
Nanotechnology  
Northwestern University

**Mario Molina**

Distinguished Professor, Chemistry and  
Biochemistry  
University of California, San Diego  
Professor, Center for Atmospheric Sciences  
at the Scripps Institution of Oceanography

**Staff****Marjory S. Blumenthal**

Executive Director

**Ashley Predith**

Assistant Executive Director

**Knatokie Ford**

AAAS Science & Technology Policy Fellow

**Craig Mundie**

Senior Advisor to the CEO  
Microsoft Corporation

**Ed Penhoet**

Director, Alta Partners  
Professor Emeritus, Biochemistry and Public  
Health  
University of California, Berkeley

**Barbara Schaal**

Mary-Dell Chilton Distinguished Professor of  
Biology  
Washington University, St. Louis

**Eric Schmidt**

Executive Chairman  
Google, Inc.

**Daniel Schrag**

Sturgis Hooper Professor of Geology  
Professor, Environmental Science and  
Engineering  
Director, Harvard University Center for  
Environment  
Harvard University



## PCAST Big Data and Privacy Working Group

### Working Group Co-Chairs

**Susan L. Graham**

Pehong Chen Distinguished Professor  
Emerita in Electrical Engineering and  
Computer Science  
University of California, Berkeley

**William Press**

Raymer Professor in Computer Science and  
Integrative Biology  
University of Texas at Austin

### Working Group Members

**S. James Gates, Jr.**

John S. Toll Professor of Physics  
Director, Center for String and Particle  
Theory  
University of Maryland, College Park

**Eric S. Lander**

President  
Broad Institute of Harvard and MIT

**Mark Gorenberg**

Managing Member  
Zetta Venture Partners

**Craig Mundie**

Senior Advisor to the CEO  
Microsoft Corporation

**John P. Holdren**

Assistant to the President for Science and  
Technology  
Director, Office of Science and Technology  
Policy

**Maxine Savitz**

Vice President  
National Academy of Engineering

**Eric Schmidt**

Executive Chairman  
Google, Inc.

### Working Group Staff

**Marjory S. Blumenthal**

Executive Director  
President's Council of Advisors on Science  
and Technology

**Michael Johnson**

Assistant Director  
National Security and International Affairs



EXECUTIVE OFFICE OF THE PRESIDENT  
PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY  
WASHINGTON, D.C. 20502

President Barack Obama  
The White House  
Washington, DC 20502

Dear Mr. President,

We are pleased to send you this report, *Big Data and Privacy: A Technological Perspective*, prepared for you by the President's Council of Advisors on Science and Technology (PCAST). It was developed to complement and inform the analysis of big-data implications for policy led by your Counselor, John Podesta, in response to your requests of January 17, 2014. PCAST examined the nature of current technologies for managing and analyzing big data and for preserving privacy, it considered how those technologies are evolving, and it explained what the technological capabilities and trends imply for the design and enforcement of public policy intended to protect privacy in big-data contexts.

Big data drives big benefits, from innovative businesses to new ways to treat diseases. The challenges to privacy arise because technologies collect so much data (e.g., from sensors in everything from phones to parking lots) and analyze them so efficiently (e.g., through data mining and other kinds of analytics) that it is possible to learn far more than most people had anticipated or can anticipate given continuing progress. These challenges are compounded by limitations on traditional technologies used to protect privacy (such as de-identification). PCAST concludes that technology alone cannot protect privacy, and policy intended to protect privacy needs to reflect what is (and is not) technologically feasible.

In light of the continuing proliferation of ways to collect and use information about people, PCAST recommends that policy focus primarily on whether specific *uses* of information about people affect privacy adversely. It also recommends that policy focus on outcomes, on the "what" rather than the "how," to avoid becoming obsolete as technology advances. The policy framework should accelerate the development and commercialization of technologies that can help to contain adverse impacts on privacy, including research into new technological options. By using technology more effectively, the Nation can lead internationally in making the most of big data's benefits while limiting the concerns it poses for privacy. Finally, PCAST calls for efforts to assure that there is enough talent available with the expertise needed to develop and use big data in a privacy-sensitive way.

PCAST is grateful for the opportunity to serve you and the country in this way and hope that you and others who read this report find our analysis useful.

Best regards,



John P. Holdren  
Co-chair, PCAST



Eric S. Lander  
Co-chair, PCAST







## Table of Contents

The President's Council of Advisors on Science and Technology .....	i
PCAST Big Data and Privacy Working Group .....	ii
Table of Contents .....	vii
Executive Summary .....	ix
1. Introduction .....	1
1.1 Context and outline of this report .....	1
1.2 Technology has long driven the meaning of privacy .....	3
1.3 What is different today? .....	5
1.4 Values, harms, and rights .....	6
2. Examples and Scenarios .....	11
2.1 Things happening today or very soon .....	11
2.2 Scenarios of the near future in healthcare and education .....	13
2.2.1 Healthcare: personalized medicine .....	13
2.2.2 Healthcare: detection of symptoms by mobile devices .....	13
2.2.3 Education .....	14
2.3 Challenges to the home's special status .....	14
2.4 Tradeoffs among privacy, security, and convenience .....	17
3. Collection, Analytics, and Supporting Infrastructure .....	19
3.1 Electronic sources of personal data .....	19
3.1.1 "Born digital" data .....	19
3.1.2 Data from sensors .....	22
3.2 Big data analytics .....	24
3.2.1 Data mining .....	24
3.2.2 Data fusion and information integration .....	25
3.2.3 Image and speech recognition .....	26
3.2.4 Social-network analysis .....	28
3.3 The infrastructure behind big data .....	30
3.3.1 Data centers .....	30
3.3.2 The cloud .....	31
4. Technologies and Strategies for Privacy Protection .....	33
4.1 The relationship between cybersecurity and privacy .....	33
4.2 Cryptography and encryption .....	35

BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

4.2.1 Well Established encryption technology.....	35
4.2.2 Encryption frontiers.....	36
4.3 Notice and consent.....	38
4.4 Other strategies and techniques.....	38
4.4.1 Anonymization or de-identification.....	38
4.4.2 Deletion and non-retention.....	39
4.5 Robust technologies going forward.....	40
4.5.1 A Successor to Notice and Consent.....	40
4.5.2 Context and Use.....	41
4.5.3 Enforcement and deterrence.....	42
4.5.4 Operationalizing the Consumer Privacy Bill of Rights.....	43
5. PCAST Perspectives and Conclusions.....	47
5.1 Technical feasibility of policy interventions.....	48
5.2 Recommendations.....	49
5.4 Final Remarks.....	53
Appendix A. Additional Experts Providing Input.....	55
Special Acknowledgment.....	57



## Executive Summary

The ubiquity of computing and electronic communication technologies has led to the exponential growth of data from both digital and analog sources. New capabilities to gather, analyze, disseminate, and preserve vast quantities of data raise new concerns about the nature of privacy and the means by which individual privacy might be compromised or protected.

After providing an overview of this report and its origins, Chapter 1 describes the changing nature of privacy as computing technology has advanced and big data has come to the fore. The term privacy encompasses not only the famous “right to be left alone,” or keeping one’s personal matters and relationships secret, but also the ability to share information selectively but not publicly. Anonymity overlaps with privacy, but the two are not identical. Likewise, the ability to make intimate personal decisions without government interference is considered to be a privacy right, as is protection from discrimination on the basis of certain personal characteristics (such as race, gender, or genome). Privacy is not just about secrets.

Conflicts between privacy and new technology have occurred throughout American history. Concern with the rise of mass media such as newspapers in the 19<sup>th</sup> century led to legal protections against the harms or adverse consequences of “intrusion upon seclusion,” public disclosure of private facts, and unauthorized use of name or likeness in commerce. Wire and radio communications led to 20<sup>th</sup> century laws against wiretapping and the interception of private communications – laws that, PCAST notes, have not always kept pace with the technological realities of today’s digital communications.

Past conflicts between privacy and new technology have generally related to what is now termed “small data,” the collection and use of data sets by private- and public-sector organizations where the data are disseminated in their original form or analyzed by conventional statistical methods. Today’s concerns about big data reflect both the substantial increases in the amount of data being collected and associated changes, both actual and potential, in how they are used.

Big data is big in two different senses. It is big in the quantity and variety of data that are available to be processed. And, it is big in the scale of analysis (termed “analytics”) that can be applied to those data, ultimately to make inferences and draw conclusions. By data mining and other kinds of analytics, non-obvious and sometimes private information can be derived from data that, at the time of their collection, seemed to raise no, or only manageable, privacy issues. Such new information, used appropriately, may often bring benefits to individuals and society – Chapter 2 of this report gives many such examples, and additional examples are scattered throughout the rest of the text. Even in principle, however, one can never know what information may later be extracted from any particular collection of big data, both because that information may result only from the combination of seemingly unrelated data sets, and because the algorithm for revealing the new information may not even have been invented at the time of collection.

The same data and analytics that provide benefits to individuals and society if used appropriately can also create potential harms – threats to individual privacy according to privacy norms both widely

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

shared and personal. For example, large-scale analysis of research on disease, together with health data from electronic medical records and genomic information, might lead to better and timelier treatment for individuals but also to inappropriate disqualification for insurance or jobs. GPS tracking of individuals might lead to better community-based public transportation facilities, but also to inappropriate use of the whereabouts of individuals. A list of the kinds of adverse consequences or harms from which individuals should be protected is proposed in Section 1.4. PCAST believes strongly that the positive benefits of big-data technology are (or can be) greater than any new harms.

Chapter 3 of the report describes the many new ways in which personal data are acquired, both from original sources, and through subsequent processing. Today, although they may not be aware of it, individuals constantly emit into the environment information whose use or misuse may be a source of privacy concerns. Physically, these information emanations are of two types, which can be called “born digital” and “born analog.”

When information is “born digital,” it is created, by us or by a computer surrogate, specifically for use by a computer or data processing system. When data are born digital, privacy concerns can arise from over-collection. Over-collection occurs when a program’s design intentionally, and sometimes clandestinely, collects information unrelated to its stated purpose. Over-collection can, in principle, be recognized at the time of collection.

When information is “born analog,” it arises from the characteristics of the physical world. Such information becomes accessible electronically when it impinges on a sensor such as a camera, microphone, or other engineered device. When data are born analog, they are likely to contain more information than the minimum necessary for their immediate purpose, and for valid reasons. One reason is for robustness of the desired “signal” in the presence of variable “noise.” Another is technological convergence, the increasing use of standardized components (e.g., cell-phone cameras) in new products (e.g., home alarm systems capable of responding to gesture).

Data fusion occurs when data from different sources are brought into contact and new facts emerge (see Section 3.2.2). Individually, each data source may have a specific, limited purpose. Their combination, however, may uncover new meanings. In particular, data fusion can result in the identification of individual people, the creation of profiles of an individual, and the tracking of an individual’s activities. More broadly, data analytics discovers patterns and correlations in large corpuses of data, using increasingly powerful statistical algorithms. If those data include personal data, the inferences flowing from data analytics may then be mapped back to inferences, both certain and uncertain, about individuals.

Because of data fusion, privacy concerns may not necessarily be recognizable in born-digital data when they are collected. Because of signal-processing robustness and standardization, the same is true of born-analog data – even data from a single source (e.g., a single security camera). Born-digital and born-analog data can both be combined with data fusion, and new kinds of data can be generated from data analytics. The beneficial uses of near-ubiquitous data collection are large, and they fuel an increasingly important set of economic activities. Taken together, these considerations suggest that a policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one



## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).

If collection cannot, in most cases, be limited practically, then what? Chapter 4 discusses in detail a number of technologies that have been used in the past for privacy protection, and others that may, to a greater or lesser extent, serve as technology building blocks for future policies.

Some technology building blocks (for example, cybersecurity standards, technologies related to encryption, and formal systems of auditable access control) are already being utilized and need to be encouraged in the marketplace. On the other hand, some techniques for privacy protection that have seemed encouraging in the past are useful as supplementary ways to reduce privacy risk, but do not now seem sufficiently robust to be a dependable basis for privacy protection where big data is concerned. For a variety of reasons, PCAST judges anonymization, data deletion, and distinguishing data from metadata (defined below) to be in this category. The framework of notice and consent is also becoming unworkable as a useful foundation for policy.

Anonymization is increasingly easily defeated by the very techniques that are being developed for many legitimate applications of big data. In general, as the size and diversity of available data grows, the likelihood of being able to re-identify individuals (that is, re-associate their records with their names) grows substantially. While anonymization may remain somewhat useful as an added safeguard in some situations, approaches that deem it, by itself, a sufficient safeguard need updating.

While it is good business practice that data of all kinds should be deleted when they are no longer of value, economic or social value often can be obtained from applying big data techniques to masses of data that were otherwise considered to be worthless. Similarly, archival data may also be important to future historians, or for later longitudinal analysis by academic researchers and others. As described above, many sources of data contain latent information about individuals, information that can be known only if the holder expends analytic resources, or that may become knowable only in the future with the development of new data-mining algorithms. In such cases it is practically impossible for the data holder even to surface “all the data about an individual,” much less delete it on any specified schedule or in response to an individual’s request. Today, given the distributed and redundant nature of data storage, it is not even clear that data, even small data, *can* be destroyed with any high degree of assurance.

As data sets become more complex, so do the attached metadata. Metadata are ancillary data that describe properties of the data such as the time the data were created, the device on which they were created, or the destination of a message. Included in the data or metadata may be identifying information of many kinds. It cannot today generally be asserted that metadata raise fewer privacy concerns than data.

Notice and consent is the practice of requiring individuals to give positive consent to the personal data collection practices of each individual app, program, or web service. Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent.

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

The conceptual problem with notice and consent is that it fundamentally places the burden of privacy protection on the individual. Notice and consent creates a non-level playing field in the implicit privacy negotiation between provider and user. The provider offers a complex, take-it-or-leave-it set of terms, while the user, in practice, can allocate only a few seconds to evaluating the offer. This is a kind of market failure.

PCAST believes that the responsibility for using personal data in accordance with the user's preferences should rest with the provider rather than with the user. As a practical matter, in the private sector, third parties chosen by the consumer (e.g., consumer-protection organizations, or large app stores) could intermediate: A consumer might choose one of several "privacy protection profiles" offered by the intermediary, which in turn would vet apps against these profiles. By vetting apps, the intermediaries would create a marketplace for the negotiation of community standards for privacy. The Federal government could encourage the development of standards for electronic interfaces between the intermediaries and the app developers and vendors.

After data are collected, data analytics come into play and may generate an increasing fraction of privacy issues. Analysis, per se, does not directly touch the individual (it is neither collection nor, without additional action, use) and may have no external visibility. By contrast, it is the *use* of a product of analysis, whether in commerce, by government, by the press, or by individuals, that can cause adverse consequences to individuals.

More broadly, PCAST believes that it is the use of data (including born-digital or born-analog data and the products of data fusion and analysis) that is the locus where consequences are produced. This locus is the technically most feasible place to protect privacy. Technologies are emerging, both in the research community and in the commercial world, to describe privacy policies, to record the origins (provenance) of data, their access, and their further use by programs, including analytics, and to determine whether those uses conform to privacy policies. Some approaches are already in practical use.

Given the statistical nature of data analytics, there is uncertainty that discovered properties of groups apply to a particular individual in the group. Making incorrect conclusions about individuals may have adverse consequences for them and may affect members of certain groups disproportionately (e.g., the poor, the elderly, or minorities). Among the technical mechanisms that can be incorporated in a use-based approach are methods for imposing standards for data accuracy and integrity and policies for incorporating useable interfaces that allow an individual to correct the record with voluntary additional information.

PCAST's charge for this study did not ask it to recommend specific privacy policies, but rather to make a relative assessment of the technical feasibilities of different broad policy approaches. Chapter 5, accordingly, discusses the implications of current and emerging technologies for government policies for privacy protection. The use of technical measures for enforcing privacy can be stimulated by reputational pressure, but such measures are most effective when there are regulations and laws with civil or criminal penalties. Rules and regulations provide both deterrence of harmful actions and incentives to deploy privacy-protecting technologies. Privacy protection cannot be achieved by technical measures alone.

This discussion leads to five recommendations.

**Recommendation 1. Policy attention should focus more on the actual uses of big data and less on its collection and analysis.** By actual uses, we mean the specific events where something happens that can cause an adverse consequence or harm to an individual or class of individuals. In the context of big data, these events (“uses”) are almost always actions of a computer program or app interacting either with the raw data or with the fruits of analysis of those data. In this formulation, it is not the data themselves that cause the harm, nor the program itself (absent any data), but the confluence of the two. These “use” events (in commerce, by government, or by individuals) embody the necessary specificity to be the subject of regulation. By contrast, PCAST judges that policies focused on the regulation of data collection, storage, retention, a priori limitations on applications, and analysis (absent identifiable actual uses of the data or products of analysis) are unlikely to yield effective strategies for improving privacy. Such policies would be unlikely to be scalable over time, or to be enforceable by other than severe and economically damaging measures.

**Recommendation 2. Policies and regulation, at all levels of government, should not embed particular technological solutions, but rather should be stated in terms of intended outcomes.**

To avoid falling behind the technology, it is essential that policy concerning privacy protection should address the purpose (the “what”) rather than prescribing the mechanism (the “how”).

**Recommendation 3. With coordination and encouragement from OSTP,<sup>1</sup> the NITRD agencies<sup>2</sup> should strengthen U.S. research in privacy-related technologies and in the relevant areas of social science that inform the successful application of those technologies.**

Some of the technology for controlling uses already exists. However, research (and funding for it) is needed in the technologies that help to protect privacy, in the social mechanisms that influence privacy-preserving behavior, and in the legal options that are robust to changes in technology and create appropriate balance among economic opportunity, national priorities, and privacy protection.

**Recommendation 4. OSTP, together with the appropriate educational institutions and professional societies, should encourage increased education and training opportunities concerning privacy protection, including career paths for professionals.**

Programs that provide education leading to privacy expertise (akin to what is being done for security expertise) are essential and need encouragement. One might envision careers for digital-privacy experts both on the software development side and on the technical management side.

---

<sup>1</sup> The White House Office of Science and Technology Policy

<sup>2</sup> NITRD refers to the Networking and Information Technology Research and Development program, whose participating Federal agencies support unclassified research in advanced information technologies such as computing, networking, and software and include both research- and mission-focused agencies such as NSF, NIH, NIST, DARPA, NOAA, DOE’s Office of Science, and the DOD military-service laboratories (see [http://www.nitrd.gov/SUBCOMMITTEE/nitrd\\_agencies/index.aspx](http://www.nitrd.gov/SUBCOMMITTEE/nitrd_agencies/index.aspx)).



## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

**Recommendation 5. The United States should take the lead both in the international arena and at home by adopting policies that stimulate the use of practical privacy-protecting technologies that exist today. It can exhibit leadership both by its convening power (for instance, by promoting the creation and adoption of standards) and also by its own procurement practices (such as its own use of privacy-preserving cloud services).**

PCAST is not aware of more effective innovation or strategies being developed abroad; rather, some countries seem inclined to pursue what PCAST believes to be blind alleys. This circumstance offers an opportunity for U.S. technical leadership in privacy in the international arena, an opportunity that should be taken.



## 1. Introduction

In a widely noted speech on January 17, 2014, President Barack Obama charged his Counselor, John Podesta, with leading a comprehensive review of big data and privacy, one that would “reach out to privacy experts, technologists, and business leaders and look at how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security.”<sup>3</sup> The President and Counselor Podesta asked the President’s Council of Advisors on Science and Technology (PCAST) to assist with the technology dimensions of the review.

For this task PCAST’s statement of work reads, in part,

PCAST will study the technological aspects of the intersection of big data with individual privacy, in relation to both the current state and possible future states of the relevant technological capabilities and associated privacy concerns.

Relevant big data include data and metadata collected, or potentially collectable, from or about individuals by entities that include the government, the private sector, and other individuals. It includes both proprietary and open data, and also data about individuals collected incidentally or accidentally in the course of other activities (e.g., environmental monitoring or the “Internet of Things”).

This is a tall order, especially on the ambitious timescale requested by the President. The literature and public discussion of big data and privacy are vast, with new ideas and insights generated daily from a variety of constituencies: technologists in industry and academia, privacy and consumer advocates, legal scholars, and journalists (among others). Independently of PCAST, but informing this report, the Podesta study sponsored three public workshops at universities across the country. Limiting this report’s charge to technological, not policy, aspects of the problem narrows PCAST’s mandate somewhat, but this is a subject where technology and policy are difficult to separate. In any case, it is the nature of the subject that this report must be regarded as based on a momentary snapshot of the technology, although we believe the key conclusions and recommendations have lasting value.

### 1.1 Context and outline of this report

The ubiquity of computing and electronic communication technologies has led to the exponential growth of online data, from both digital and analog sources. New technological capabilities to create, analyze, and disseminate vast quantities of data raise new concerns about the nature of privacy and the means by which individual privacy might be compromised or protected.

This report discusses present and future technologies concerning this so-called “big data” as it relates to privacy concerns. It is not a complete summary of the technology concerning big data, nor a complete summary of the ways in which technology affects privacy, but focuses on the ways in which big-data and privacy interact. As an example, if Leslie confides a secret to Chris and Chris broadcasts that secret by email or texting, that might be a

<sup>3</sup> “Remarks by the President on Review of Signals Intelligence,” January 17, 2014. <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

privacy-infringing use of information technology, but it is not a big-data issue. As another example, if oceanographic data are collected in large quantities by remote sensing, that is big data, but not, in the first instance, a privacy concern. Some data are more privacy-sensitive than others, for example, personal medical data, as distinct from personal data publicly shared by the same individual. Different technologies and policies will apply to different classes of data.

The notions of big data and the notions of individual privacy used in this report are intentionally broad and inclusive. Business consultants Gartner, Inc. define big data as “high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making,”<sup>4</sup> while computer scientists reviewing multiple definitions offer the more technical, “a term describing the storage and analysis of large and/or complex data sets using a series of techniques including, but not limited to, NoSQL, MapReduce, and machine learning.”<sup>5</sup> (See Sections 3.2.1 and 3.3.1 for discussion of these technical terms.) In a privacy context, the term “big data” typically means data about one or a group of individuals, or that might be analyzed to make inferences about individuals. It might include data or metadata collected by government, by the private sector, or by individuals. The data and metadata might be proprietary or open, they might be collected intentionally or incidentally or accidentally. They might be text, audio, video, sensor-based, or some combination. They might be data collected directly from some source, or data derived by some process of analysis. They might be saved for a long period of time, or they might be analyzed and discarded as they are streamed. In this report, PCAST usually does not distinguish between “data” and “information.”

The term “privacy” encompasses not only avoiding observation, or keeping one’s personal matters and relationships secret, but also the ability to share information selectively but not publicly. Anonymity overlaps with privacy, but the two are not identical. Voting is recognized as private, but not anonymous, while authorship of a political tract may be anonymous, but it is not private. Likewise, the ability to make intimate personal decisions without government interference is considered to be a privacy right, as is protection from discrimination on the basis of certain personal characteristics (such as an individual’s race, gender, or genome). So, privacy is not just about secrets.

The promise of big-data collection and analysis is that the derived data can be used for purposes that benefit both individuals and society. Threats to privacy stem from the deliberate or inadvertent disclosure of collected or derived individual data, the misuse of the data, and the fact that derived data may be inaccurate or false. The technologies that address the confluence of these issues are the subject of this report.<sup>6</sup>

The remainder of this introductory chapter gives further context in the form of a summary of how the legal concept of privacy developed historically in the United States. Interestingly, and relevant to this report, privacy rights and the development of new technologies have long been intertwined. Today’s issues are no exception.

Chapter 2 of this report is devoted to scenarios and examples, some from today, but most anticipating a near tomorrow. Yogi Berra’s much-quoted remark – “It’s tough to make predictions, especially about the future” – is

---

<sup>4</sup> Gartner, Inc., “IT Glossary,” <https://www.gartner.com/it-glossary/big-data/>

<sup>5</sup> Barker, Adam and Jonathan Stuart Ward, “Undefined By Data: A Survey of Big Data Definitions,” arXiv:1309.5821. <http://arxiv.org/abs/1309.5821>

<sup>6</sup> PCAST acknowledges gratefully the assistance of several contributors at the National Science Foundation, who helped to identify and distill key insights from the technical literature and research community, as well as other technical experts in academia and industry that it consulted during this project. See Appendix A.

germane. But it is equally true for this subject that policies based on out-of-date examples and scenarios are doomed to failure. Big-data technologies are advancing so rapidly that predictions about the future, however imperfect, must guide today's policy development.

Chapter 3 examines the technology dimensions of the two great pillars of big data: collection and analysis. In a certain sense big data is exactly the confluence of these two: big collection meets big analysis (often termed "analytics"). The technical infrastructure of large-scale networking and computing that enables "big" is also discussed.

Chapter 4 looks at technologies and strategies for the protection of privacy. Although technology may be part of the problem, it must also be part of the solution. Many current and foreseeable technologies can enhance privacy, and there are many additional promising avenues of research.

Chapter 5, drawing on the previous chapters, contains PCAST's perspectives and conclusions. While it is not within this report's charge to recommend specific policies, it is clear that certain kinds of policies are technically more feasible and less likely to be rendered irrelevant or unworkable by new technologies than others. These approaches are highlighted, along with comments on the technical deficiencies of some other approaches. This chapter also contains PCAST's recommendations in areas that lie within our charge, that is, other than policy.

## 1.2 Technology has long driven the meaning of privacy

The conflict between privacy and new technology is not new, except perhaps now in its greater scope, degree of intimacy, and pervasiveness. For more than two centuries, values and expectations relating to privacy have been continually reinterpreted and rearticulated in light of the impact of new technologies.

The nationwide postal system advocated by Benjamin Franklin and established in 1775 was a new technology designed to promote interstate commerce. But mail was routinely and opportunistically opened in transit until Congress made this action illegal in 1782. While the Constitution's Fourth Amendment codified the heightened privacy protection afforded to people in their homes or on their persons (previously principles of British common law), it took another century of technological challenges to expand the concept of privacy rights into more abstract spaces, including the electronic. The invention of the telegraph and, later, telephone created new tensions that were slow to be resolved. A bill to protect the privacy of telegrams, introduced in Congress in 1880, was never passed.<sup>7</sup>

It was not telecommunications, however, but the invention of the portable, consumer-operable camera (soon known as the Kodak) that gave impetus to Warren and Brandeis's 1890 article "The Right to Privacy,"<sup>8</sup> then a controversial title, but now viewed as the foundational document for modern privacy law. In the article, Warren and Brandeis gave voice to the concern that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops,'" further noting that "[f]or years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons..."<sup>9</sup>

<sup>7</sup> Seipp, David J., *The Right to Privacy in American History*, Harvard University, Program on Information Resources Policy, Cambridge, MA, 1978.

<sup>8</sup> Warren, Samuel D. and Louis D. Brandeis, "The Right to Privacy." *Harvard Law Review* 4:5, 193, December 15, 1890.

<sup>9</sup> *Id.* at 195.

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

Warren and Brandeis sought to articulate the right of privacy between individuals (whose foundation lies in civil tort law). Today, many states recognize a number of privacy-related harms as causes for civil or criminal legal action (further discussed in Section 1.4).<sup>10</sup>

From Warren and Brandeis' "right to privacy," it took another 75 years for the Supreme Court to find, in *Griswold v. Connecticut*<sup>11</sup> (1965), a right to privacy in the "penumbras" and "emanations" of other constitutional protections (as Justice William O. Douglas put it, writing for the majority).<sup>12</sup> With a broad perspective, scholars today recognize a number of different legal meanings for "privacy." Five of these seem particularly relevant to this PCAST report:

- (1) The individual's right to keep secrets or seek seclusion (the famous "right to be left alone" of Brandeis' 1928 dissenting opinion in *Olmstead v. United States*).<sup>13</sup>
- (2) The right to anonymous expression, especially (but not only) in political speech (as in *McIntyre v. Ohio Elections Commission*)<sup>14</sup>
- (3) The ability to control access by others to personal information after it leaves one's exclusive possession (for example, as articulated in the FTC's Fair Information Practice Principles).<sup>15</sup>
- (4) The barring of some kinds of negative consequences from the use of an individual's personal information (for example, job discrimination on the basis of personal DNA, forbidden in 2008 by the Genetic Information Nondiscrimination Act<sup>16</sup>).
- (5) The right of the individual to make intimate decisions without government interference, as in the domains of health, reproduction, and sexuality (as in *Griswold*).

These are asserted, not absolute, rights. All are supported, but also circumscribed, by both statute and case law. With the exception of number 5 on the list (a right of "decisional privacy" as distinct from "informational privacy"), all are applicable in varying degrees both to citizen-government interactions and to citizen-citizen interactions. Collisions between new technologies and privacy rights have occurred in all five. A patchwork of state and federal laws have addressed concerns in many sectors, but to date there has not been comprehensive legislation to handle these issues. Collisions between new technologies and privacy rights should be expected to continue to occur.

---

<sup>10</sup> Digital Media Law Project, "Publishing Personal and Private Information." <http://www.dmlp.org/legal-guide/publishing-personal-and-private-information>

<sup>11</sup> *Griswold v. Connecticut*, 381 U.S. 479 (1965).

<sup>12</sup> *Id.* at 483-84.

<sup>13</sup> *Olmstead v. United States*, 277 U.S. 438 (1928).

<sup>14</sup> *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 340-41 (1995). The decision reads in part, "Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views . . . Anonymity is a shield from the tyranny of the majority . . . It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society."

<sup>15</sup> Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," May 2000.

<sup>16</sup> Genetic Information Nondiscrimination Act of 2008, PL 110-233, May 21, 2008, 122 Stat 881.

### 1.3 What is different today?

New collisions between technologies and privacy have become evident, as new technological capabilities have emerged at a rapid pace. It is no longer clear that the five privacy concerns raised above, or their current legal interpretations, are sufficient in the court of public opinion.

Much of the public's concern is with the harm done by the use of personal data, both in isolation or in combination. Controlling access to personal data after they leave one's exclusive possession has been seen historically as a means of controlling potential harm. But today, personal data may never be, or have been, within one's possession – for instance they may be acquired passively from external sources such as public cameras and sensors, or without one's knowledge from public electronic disclosures by others using social media. In addition, personal data may be derived from powerful data analyses (see Section 3.2) whose use and output is unknown to the individual. Those analyses sometimes yield valid conclusions that the individual would not want disclosed. Worse yet, the analyses can produce false positives or false negatives -- information that is a consequence of the analysis but is not true or correct. Furthermore, to a much greater extent than before, the same personal data have both beneficial and harmful uses, depending on the purposes for which and the contexts in which they are used. Information supplied by the individual might be used only to derive other information such as identity or a correlation, after which it is not needed. The derived data, which were never under the individual's control, might then be used either for good or ill.

In the current discourse, some assert that the issues concerning privacy protection are collective as well as individual, particularly in the domain of civil rights – for example, identification of certain individuals at a gathering using facial recognition from videos, and the inference that other individuals at the same gathering, also identified from videos, have similar opinions or behaviors.

Current circumstances also raise issues of how the right to privacy extends to the public square, or to quasi-private gatherings such as parties or classrooms. If the observers in these venues are not just people, but also both visible and invisible recording devices with enormous fidelity and easy paths to electronic promulgation and analysis, does that change the rules?

Also rapidly changing are the distinctions between government and the private sector as potential threats to individual privacy. Government is not just a “giant corporation.” It has a monopoly in the use of force; it has no direct competitors who seek market advantage over it and may thus motivate it to correct missteps. Governments have checks and balances, which can contribute to self-imposed limits on what they may do with people's information. Companies decide how they will use such information in the context of such factors as competitive advantages and risks, government regulation, and perceived threats and consequences of lawsuits. It is thus appropriate that there are different sets of constraints on the public and private sectors. But government has a set of authorities – particularly in the areas of law enforcement and national security – that place it in a uniquely powerful position, and therefore the restraints placed on its collection and use of data deserve special attention. Indeed, the need for such attention is heightened because of the increasingly blurry line between public and private data.

While these differences are real, big data is to some extent a leveler of the differences between government and companies. Both governments and companies have potential access to the same sources of data and the same analytic tools. Current rules may allow government to purchase or otherwise obtain data from the private

sector that, in some cases, it could not legally collect itself,<sup>17</sup> or to outsource to the private sector analyses it could not itself legally perform.<sup>18</sup> The possibility of government exercising, without proper safeguards, its own monopoly powers and also having unfettered access to the private information marketplace is unsettling.

What kinds of actions should be forbidden both to government (Federal, state, and local, and including law enforcement) and to the private sector? What kinds should be forbidden to one but not the other? It is unclear whether current legal frameworks are sufficiently robust for today's challenges.

#### 1.4 Values, harms, and rights

As was seen in Sections 1.2 and 1.3, new privacy rights usually do not come into being as academic abstractions. Rather, they arise when technology encroaches on widely shared values. Where there is consensus on values, there can also be consensus on what kinds of harms to individuals may be an affront to those values. Not all such harms may be preventable or remediable by government actions, but, conversely, it is unlikely that government actions will be welcome or effective if they are not grounded to some degree in values that are widely shared.

In the realm of privacy, Warren and Brandeis in 1890<sup>19</sup> (see Section 1.2) began a dialogue about privacy that led to the evolution of the right in academia and the courts, later crystalized by William Prosser as four distinct harms that had come to earn legal protection.<sup>20</sup> A direct result is that, today, many states recognize as causes for legal action the four harms that Prosser enumerated,<sup>21</sup> and which have become (though varying from state to state<sup>22</sup>) privacy "rights." The harms are:

- Intrusion upon seclusion. A person who intentionally intrudes, physically or otherwise (now including electronically), upon the solitude or seclusion of another person or her private affairs or concerns, can be subject to liability for the invasion of her privacy, but only if the intrusion would be highly offensive to a reasonable person.
- Public disclosure of private facts. Similarly, a person can be sued for publishing private facts about another person, even if those facts are true. Private facts are those about someone's personal life that have not previously been made public, that are not of legitimate public concern, and that would be offensive to a reasonable person.

<sup>17</sup> One Hundred Tenth Congress, "Privacy: The use of commercial information resellers by federal agencies," *Hearing before the Subcommittee on Information Policy, Census, and National Archives of the Committee on Oversight and Government Reform*, House of Representatives, March 11, 2008.

<sup>18</sup> For example, Experian provides much of Healthcare.gov's identity verification component using consumer credit information not available to the government. See *Consumer Reports*, "Having trouble proving your identity to HealthCare.gov? Here's how the process works," December 18, 2013.

<http://www.consumerreports.org/cro/news/2013/12/how-to-prove-your-identity-on-healthcare.gov/index.htm?loginMethod=auto>

<sup>19</sup> Warren, Samuel D. and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4:5, 193, December 15, 1890.

<sup>20</sup> Prosser, William L., "Privacy," *California Law Review* 48:383, 389, 1960.

<sup>21</sup> *Id.*

<sup>22</sup> (1) Digital Media Law Project, "Publishing Personal and Private Information." <http://www.dmlp.org/legal-guide/publishing-personal-and-private-information>. (2) *Id.*, "Elements of an Intrusion Claim." <http://www.dmlp.org/legal-guide/elements-intrusion-claim>

- “False light” or publicity. Closely related to defamation, this harm results when false facts are widely published about an individual. In some states, false light includes untrue implications, not just untrue facts as such.
- Misappropriation of name or likeness. Individuals have a “right of publicity” to control the use of their name or likeness in commercial settings.

It seems likely that most Americans today continue to share the values implicit in these harms, even if the legal language (by now refined in thousands of court decisions) strikes one as archaic and quaint. However, new technological insults to privacy, actual or prospective, and a century’s evolution of social values (for example, today’s greater recognition of the rights of minorities, and of rights associated with gender), may require a longer list than sufficed in 1960.

Although PCAST’s engagement with this subject is centered on technology, not law, any report on the subject of privacy, including PCAST’s, should be grounded in the values of its day. As a starting point for discussion, albeit only a snapshot of the views of one set of technologically minded Americans, PCAST offers some possible augmentations to the established list of harms, each of which suggests a possible underlying right in the age of big data.

PCAST also believes strongly that the positive benefits of technology are (or can be) greater than any new harms. Almost every new harm is related to or “adjacent to” beneficial uses of the same technology.<sup>23</sup> To emphasize this point, for each suggested new harm, we describe a related beneficial use.

- **Invasion of private communications.** Digital communications technologies make social networking possible across the boundaries of geography, and enable social and political participation on previously unimaginable scales. An individual’s right to private communication, secured for written mail and wireline telephone in part by the isolation of their delivery infrastructure, may need reaffirmation in the digital era, however, where all kinds of “bits” share the same pipelines, and the barriers to interception are often much lower. (In this context, we discuss the use and limitations of encryption in Section 4.2.)
- **Invasion of privacy in a person’s virtual home.** The Fourth Amendment gives special protection against government intrusion into the home, for example the protection of private records within the home; tort law offers protection against similar non-government intrusion. The new “virtual home” includes the Internet, cloud storage, and other services. Personal data in the cloud can be accessible and organized. Photographs and records in the cloud can be shared with family and friends, and can be passed down to future generations. The underlying social value, the “home as one’s castle,” should logically extend to one’s “castle in the cloud,” but this protection has not been preserved in the new virtual home. (We discuss this subject further in Section 2.3.)
- **Public disclosure of inferred private facts.** Powerful data analytics may infer personal facts from seemingly harmless input data. Sometimes the inferences are beneficial. At its best, targeted advertising directs consumers to products that they actually want or need. Inferences about people’s health can lead to better and timelier treatments and longer lives. But before the advent of big data, it could be assumed that there was a clear distinction between public and private information: either a fact was “out there” (and could be pointed to), or it was not. Today, analytics may discover facts that

---

<sup>23</sup> One perspective informed by new technologies and technology-mediated communication suggests that privacy is about the “continual management of boundaries between different spheres of action and degrees of disclosure within those spheres,” with privacy and one’s public face being balanced in different ways at different times. See: Leysia Palen and Paul Dourish, “Unpacking ‘Privacy’ for a Networked World,” *Proceedings of CHI 2003*, Association for Computing Machinery, April 5-10, 2003.



## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

are no less private than yesterday's purely private sphere of life. Examples include inferring sexual preference from purchasing patterns, or early Alzheimer's disease from key-click streams. In the latter case, the private fact may not even be known to the individual in question. (Section 3.2 discusses the technology behind the data analytics that makes such inferences possible.) The public disclosure of such information (and possibly also some non-public commercial uses) seems offensive to widely shared values.

- **Tracking, stalking, and violations of locational privacy.** Today's technologies easily determine an individual's current or prior location. Useful location-based services include navigation, suggesting better commuter routes, finding nearby friends, avoiding natural hazards, and advertising the availability of nearby goods and services. Sighting an individual in a public place can hardly be a private fact. When big data allows such sightings, or other kinds of passive or active data collection, to be assembled into the continuous locational track of an individual's private life, however, many Americans (including Supreme Court Justice Sotomayor, for example<sup>24</sup>) perceive a potential affront to a widely accepted "reasonable expectation of privacy."
- **Harm arising from false conclusions about individuals, based on personal profiles from big-data analytics.** The power of big data, and therefore its benefit, is often correlational. In many cases the "harms" from statistical errors are small, for example the incorrect inference of a movie preference; or the suggestion that a health issue be discussed with a physician, following from analyses that may, on average, be beneficial, even when a particular instance turns out to be a false alarm. Even when predictions are statistically valid, moreover, they may be untrue about particular individuals – and mistaken conclusions may cause harm. Society may not be willing to excuse harms caused by the uncertainties inherent in statistically valid algorithms. These harms may unfairly burden particular classes of individuals, for example, racial minorities or the elderly.
- **Foreclosure of individual autonomy or self-determination.** Data analyses about large populations can discover special cases that apply to individuals within that population. For example, by identifying differences in "learning styles," big data may make it possible to personalize education in ways that recognize every individual's potential and optimize that individual's achievement. But the projection of population factors onto individuals can be misused. It is widely accepted that individuals should be able to make their own choices and pursue opportunities that are not necessarily typical, and that no one should be denied the chance to achieve more than some statistical expectation of themselves. It would offend our values if a child's choices in video games were later used for educational tracking (for example, college admissions). Similarly offensive would be a future, akin to Philip K. Dick's science fiction short story adapted by Steven Spielberg in the film *Minority Report*, where "pre-crime" is statistically identified and punished.<sup>25</sup>
- **Loss of anonymity and private association.** Anonymity is not acceptable as an enabler of committing fraud, or bullying, or cyber-stalking, or improper interactions with children. Apart from wrongful behavior, however, the individual's right to choose to be anonymous is a long held American value (as, for example, the anonymous authorship of the Federalist papers). Using data to (re-) identify an individual who wishes to be anonymous (except in the case of legitimate governmental functions, such as law enforcement) is regarded as a harm. Similarly, individuals have a right of private association with groups or other individuals, and the identification of such associations may be a harm.

<sup>24</sup> "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *United States v. Jones* (10-1259), Sotomayor concurrence at <http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf>.

<sup>25</sup> Dick, Phillip K., "The Minority Report," first published in *Fantastic Universe* (1956) and reprinted in *Selected Stories of Philip K. Dick*, New York: Pantheon, 2002.

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

While in no sense is the above list intended to be complete, it does have a few intentional omissions. For example, individuals may want big data to be used “fairly,” in the sense of treating people equally, but (apart from the small number of protected classes already defined by law) it seems impossible to turn this into a right that is specific enough to be meaningful. Likewise, individuals may want the ability to know what others know about them; but that is surely not a right from the pre-digital age; and, in the current era of statistical analysis, it is not so easy to define what “know” means. This important issue is discussed in Section 3.1.2, and again taken up in chapter 5, where the attempt is to focus on actual harms done by the *use* of information, not by a concept as technically ambiguous as whether information is *known*.





## 2. Examples and Scenarios

This chapter seeks to make Chapter 1's introductory discussion more concrete by sketching some examples and scenarios. While some of these applications of technology are in use today, others comprise PCAST's technological prognostications about the near future, up to perhaps 10 years from today. Taken together the examples and scenarios are intended to illustrate both the enormous benefits that big data can provide and also the privacy challenges that may accompany these benefits.

In the following three sections, it will be useful to develop some scenarios more completely than others, moving from very brief examples of things happening today to more fully developed scenarios set in the future.

### 2.1 Things happening today or very soon

Here are some relevant examples:

- Pioneered more than a decade ago, devices mounted on utility poles are able to sense the radio stations being listened to by passing drivers, with the results sold to advertisers.<sup>26</sup>
- In 2011, automatic license-plate readers were in use by three quarters of local police departments surveyed. Within 5 years, 25% of departments expect to have them installed on all patrol cars, alerting police when a vehicle associated with an outstanding warrant is in view.<sup>27</sup> Meanwhile, civilian uses of license-plate readers are emerging, leveraging cloud platforms and promising multiple ways of using the information collected.<sup>28</sup>
- Experts at the Massachusetts Institute of Technology and the Cambridge Police Department have used a machine-learning algorithm to identify which burglaries likely were committed by the same offender, thus aiding police investigators.<sup>29</sup>
- Differential pricing (offering different prices to different customers for essentially the same goods) has become familiar in domains such as airline tickets and college costs. Big data may increase the power and prevalence of this practice and may also decrease even further its transparency.<sup>30</sup>

<sup>26</sup> ElBoghdady, Dina, "Advertisers Tune In to New Radio Gauge," *The Washington Post*, October 25, 2004.

<http://www.washingtonpost.com/wp-dyn/articles/A60013-2004Oct24.html>

<sup>27</sup> American Civil Liberties Union, "You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements," July, 2013. <https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf>

<sup>28</sup> Hardy, Quentin, "How Urban Anonymity Disappears When All Data Is Tracked," *The New York Times*, April 19, 2014.

<sup>29</sup> Rudin, Cynthia, "Predictive policing: Using Machine Learning to Detect Patterns of Crime," *Wired*, August 22, 2013. <http://www.wired.com/insights/2013/08/predictive-policing-using-machine-learning-to-detect-patterns-of-crime/>.

<sup>30</sup> (1) Schiller, Benjamin, "First Degree Price Discrimination Using Big Data," Jan. 30, 2014, Brandeis University.

[http://benjaminshiller.com/images/First\\_Degree\\_PD\\_Using\\_Big\\_Data\\_Jan\\_27,\\_2014.pdf](http://benjaminshiller.com/images/First_Degree_PD_Using_Big_Data_Jan_27,_2014.pdf) and

<http://www.forbes.com/sites/modeledbehavior/2013/09/01/will-big-data-bring-more-price-discrimination/> (2) Fisher, William W. "When Should We Permit Differential Pricing of Information?" *UCLA Law Review* 55:1, 2007.

- The UK firm FeatureSpace offers machine-learning algorithms to the gaming industry that may detect early signs of gambling addiction or other aberrant behavior among online players.<sup>31</sup>
- Retailers like CVS and AutoZone analyze their customers' shopping patterns to improve the layout of their stores and stock the products their customers want in a particular location.<sup>32</sup> By tracking cell phones, RetailNext offers bricks-and-mortar retailers the chance to recognize returning customers, just as cookies allow them to be recognized by on-line merchants.<sup>33</sup> Similar WiFi tracking technology could detect how many people are in a closed room (and in some cases their identities).
- The retailer Target inferred that a teenage customer was pregnant and, by mailing her coupons intended to be useful, unintentionally disclosed this fact to her father.<sup>34</sup>
- The author of an anonymous book, magazine article, or web posting is frequently "outed" by informal crowd sourcing, fueled by the natural curiosity of many unrelated individuals.<sup>35</sup>
- Social media and public sources of records make it easy for anyone to infer the network of friends and associates of most people who are active on the web, and many who are not.<sup>36</sup>
- Marist College in Poughkeepsie, New York, uses predictive modeling to identify college students who are at risk of dropping out, allowing it to target additional support to those in need.<sup>37</sup>
- The Durkheim Project, funded by the U.S. Department of Defense, analyzes social-media behavior to detect early signs of suicidal thoughts among veterans.<sup>38</sup>
- LendUp, a California-based startup, sought to use nontraditional data sources such as social media to provide credit to underserved individuals. Because of the challenges in ensuring accuracy and fairness, however, they have been unable to proceed.<sup>39,40</sup>

<sup>31</sup> Burn-Murdoch, John, "UK technology firm uses machine learning to combat gambling addiction," *The Guardian*, August 1, 2013. <http://www.theguardian.com/news/datablog/2013/aug/01/uk-firm-uses-machine-learning-fight-gambling-addiction>

<sup>32</sup> Clifford, Stephanie, "Using Data to Stage-Manage Paths to the Prescription Counter," *The New York Times*, June 19, 2013. <http://bits.blogs.nytimes.com/2013/06/19/using-data-to-stage-manage-paths-to-the-prescription-counter/>

<sup>33</sup> Clifford, Stephanie, "Attention, Shoppers: Store Is Tracking Your Cell," *The New York Times*, July 14, 2013.

<sup>34</sup> Duhigg, Charles, "How Companies Learn Your Secrets," *The New York Times Magazine*, February 12, 2012.

[http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0)

<sup>35</sup> Volokh, Eugene, "Outing Anonymous Bloggers," June 8, 2009. <http://www.volokh.com/2009/06/08/outing-anonymous-bloggers/>; A. Narayanan et al., "On the Feasibility of Internet-Scale Author Identification," IEEE Symposium on Security and Privacy, May 2012. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234420>

<sup>36</sup> Facebook's "The Graph API" (at <https://developers.facebook.com/docs/graph-api/>) describes how to write computer programs that can access the Facebook friends' data.

<sup>37</sup> One of four big-data applications honored by the trade journal, *Computerworld*, in 2013. King, Julia, "UN tackles socio-economic crises with big data," *Computerworld*, June 3, 2013.

[http://www.computerworld.com/s/article/print/9239643/UN\\_tackles\\_socio\\_economic\\_crises\\_with\\_big\\_data](http://www.computerworld.com/s/article/print/9239643/UN_tackles_socio_economic_crises_with_big_data)

<sup>38</sup> Ungerleider, Neal, "This May Be The Most Vital Use Of 'Big Data' We've Ever Seen," *Fast Company*, July 12, 2013.

<http://www.fastcolabs.com/3014191/this-may-be-the-most-vital-use-of-big-data-weve-ever-seen>.

<sup>39</sup> Center for Data Innovations, *100 Data Innovations*, Information Technology and Innovation Foundation, Washington, DC, January 2014. <http://www2.datainnovation.org/2014-100-data-innovations.pdf>

<sup>40</sup> Waters, Richard, "Data open doors to financial innovation," *Financial Times*, December 13, 2013.

<http://www.ft.com/intl/cms/s/2/3c59d58a-43fb-11e2-844c-00144feabdc0.html>

- Insight into the spread of hospital-acquired infections has been gained through the use of large amounts of patient data together with personal information about uninfected patients and clinical staff.<sup>41</sup>
- Individuals' heart rates can be inferred from the subtle changes in their facial coloration that occur with each beat, enabling inferences about their health and emotional state.<sup>42</sup>

## 2.2 Scenarios of the near future in healthcare and education

Here are a few examples of the kinds of scenarios that can readily be constructed.

### 2.2.1 Healthcare: personalized medicine

Not all patients who have a particular disease are alike, nor do they respond identically to treatment. Researchers will soon be able to draw on millions of health records (including analog data such as scans in addition to digital data), vast amounts of genomic information, extensive data on successful and unsuccessful clinical trials, hospital records, and so forth. In some cases they will be able to discern that among the diverse manifestations of the disease, a subset of the patients have a collection of traits that together form a variant that responds to a particular treatment regime.

Since the result of the analysis could lead to better outcomes for particular patients, it is desirable to identify those individuals in the cohort, contact them, treat their disease in a novel way, and use their experiences in advancing the research. Their data may have been gathered only anonymously, however, or it may have been de-identified.

Solutions may be provided by specific new technologies for the protection of database privacy. These may create a protected query mechanism so individuals can find out whether they are in the cohort, or provide an alert mechanism based on the cohort characteristics so that, when a medical professional sees a patient in the cohort, a notice is generated.

### 2.2.2 Healthcare: detection of symptoms by mobile devices

Many baby boomers wonder how they might detect Alzheimer's disease in themselves. What would be better to observe their behavior than the mobile device that connects them to a personal assistant in the cloud (e.g., Siri or OK Google), helps them navigate, reminds them what words mean, remembers to do things, recalls conversations, measures gait, and otherwise is in a position to detect gradual declines on traditional and novel medical indicators that might be imperceptible even to their spouses?

At the same time, any leak of such information would be a damaging betrayal of trust. What are individuals' protections against such risks? Can the inferred information about individuals' health be sold, without additional consent, to third parties (e.g., pharmaceutical companies)? What if this is a stated condition of use of

<sup>41</sup> (1) Wiens, Jenna, John Guttag, and Eric Horvitz, "A Study in Transfer Learning: Leveraging Data from Multiple Hospitals to Enhance Hospital-Specific Predictions," *Journal of the American Medical Informatics Association*, January 2014. (2) Weitzner, Daniel J., et al., "Consumer Privacy Bill of Rights and Big Data: Response to White House Office of Science and Technology Policy Request for Information," April 4, 2014.

<sup>42</sup> Frazer, Bryant, "MIT Computer Program Reveals Invisible Motion in Video," *The New York Times* video, February 27, 2013. <https://www.youtube.com/watch?v=3rWycBEHn3s>

the app? Should information go to individuals' personal physicians with their initial consent but not a subsequent confirmation?

### 2.2.3 Education

Drawing on millions of logs of online courses, including both massive open on-line courses (MOOCs) and smaller classes, it will soon be possible to create and maintain longitudinal data about the abilities and learning styles of millions of students. This will include not just broad aggregate information like grades, but fine-grained profiles of how individual students respond to multiple new kinds of teaching techniques, how much help they need to master concepts at various levels of abstraction, what their attention span is in various contexts, and so forth. A MOOC platform can record how long a student watches a particular video; how often a segment is repeated, sped up, or skipped; how well a student does on a quiz; how many times he or she misses a particular problem; and how the student balances watching content to reading a text. As the ability to present different material to different students materializes in the platforms, the possibility of blind, randomized A/B testing enables the gold standard of experimental science to be implemented at large scale in these environments.<sup>43</sup>

Similar data are also becoming available for residential classes, as learning-management systems (such as Canvas, Blackboard, or Desire2Learn) expand their roles to support innovative pedagogy. In many courses one can now get moment-by-moment tracking of the student's engagement with the course materials and correlate that engagement with the desired learning outcomes.

With this information, it will be possible not only to greatly improve education, but also to discover what skills, taught to which individuals at which points in childhood, lead to better adult performance in certain tasks, or to adult personal and economic success. While these data could revolutionize educational research, the privacy issues are complex.<sup>44</sup>

There are many privacy challenges in this vision of the future of education. Knowledge of early performance can create implicit biases<sup>45</sup> that color later instruction and counseling. There is great potential for misuse, ostensibly for the social good, in the massive ability to direct students into high- or low-potential tracks. Parents and others have access to sensitive information about children, but mechanisms rarely exist to change those permissions when the child reaches majority.

## 2.3 Challenges to the home's special status

The home has special significance as a sanctuary of individual privacy. The Fourth Amendment's list, "persons, houses, papers, and effects," puts only the physical body in the rhetorically more prominent position; and a house is often the physical container for the other three, a boundary inside of which enhanced privacy rights apply.

<sup>43</sup> For an overview of MOOCs and associated analytics opportunities, see PCAST's December 2013 letter to the President. [http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast\\_edit\\_dec-2013.pdf](http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_edit_dec-2013.pdf)

<sup>44</sup> There is also uncertainty about how to interpret applicable laws, such as the Family Educational Rights and Privacy Act (FERPA). Recent Federal guidance is intended to help clarify the situation. See: U.S. Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices," February 2014. <http://ftac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%2028February%202014%29.pdf>

<sup>45</sup> Cukier, Kenneth, and Viktor Mayer-Schoenberger, "How Big Data Will Haunt You Forever," *Quartz*, March 11, 2014. <http://qz.com/185252/how-big-data-will-haunt-you-forever-your-high-school-transcript/>

Existing interpretations of the Fourth Amendment are inadequate for the present world, however. We, along with the “papers and effects” contemplated by the Fourth Amendment, live increasingly in cyberspace, where the physical boundary of the home has little relevance. In 1980, a family’s financial records were paper documents, located perhaps in a desk drawer inside the house. By 2000, they were migrating to the hard drive of the home computer – but still within the house. By 2020, it is likely that most such records will be in the cloud, not just outside the house, but likely replicated in multiple legal jurisdictions – because cloud storage typically uses location diversity to achieve reliability. The picture is the same if one substitutes for financial records something like “political books we purchase,” or “love letters that we receive,” or “erotic videos that we watch.” Absent different policy, legislative, and judicial approaches, the physical sanctity of the home’s papers and effects is rapidly becoming an empty legal vessel.

The home is also the central locus of Brandeis’ “right to be left alone.” This right is also increasingly fragile, however. Increasingly, people bring sensors into their homes whose immediate purpose is to provide convenience, safety, and security. Smoke and carbon monoxide alarms are common, and often required by safety codes.<sup>46</sup> Radon detectors are usual in some parts of the country. Integrated air monitors that can detect and identify many different kinds of pollutants and allergens are readily foreseeable. Refrigerators may soon be able to “sniff” for gases released from spoiled food, or, as another possible path, may be able to “read” food expiration dates from radio-frequency identification (RFID) tags in the food’s packaging. Rather than today’s annoying cacophony of beeps, tomorrow’s sensors (as some already do today) will interface to a family through integrated apps on mobile devices or display screens. The data will have been processed and interpreted. Most likely that processing will occur in the cloud. So, to deliver services the consumer wants, much data will need to have left the home.

Environmental sensors that enable new food and air safety may also be able to detect and characterize tobacco or marijuana smoke. Health care or health insurance providers may want assurance that self-declared non-smokers are telling the truth. Might they, as a condition of lower premiums, require the homeowner’s consent for tapping into the environmental monitors’ data? If the monitor detects heroin smoking, is an insurance company obligated to report this to the police? Can the insurer cancel the homeowner’s property insurance?

To some, it seems farfetched that the typical home will foreseeably acquire cameras and microphones in every room, but that appears to be a likely trend. What can your cell phone (already equipped with front and back cameras) hear or see when it is on the nightstand next to your bed? Tablets, laptops, and many desktop computers have cameras and microphones. Motion detector technology for home intrusion alarms will likely move from ultrasound and infrared to imaging cameras – with the benefit of fewer false alarms and the ability to distinguish pets from people. Facial-recognition technology will allow further security and convenience. For the safety of the elderly, cameras and microphones will be able to detect falls or collapses, or calls for help, and be networked to summon aid.

People naturally communicate by voice and gesture. It is inevitable that people will communicate with their electronic servants in both such modes (necessitating that they have access to cameras and microphones).

---

<sup>46</sup> Nest, acquired by Google, attracted attention early for its design and its use of big data to adapt to consumer behavior. See: Aoki, Kenji, “Nest Gives the Lowly Smoke Detector a Brain,” *Wired*, October, 2013. <http://www.wired.com/2013/10/nest-smoke-detector/all/>



Companies such as PrimeSense, an Israeli firm recently bought by Apple,<sup>47</sup> are developing sophisticated computer-vision software for gesture reading, already a key feature in the consumer computer game console market (e.g., Microsoft Kinect). Consumer televisions are already among the first “appliances” to respond to gesture; already, devices such as the Nest smoke detector respond to gestures.<sup>48</sup> The consumer who taps his temple to signal a spoken command to Google Glass<sup>49</sup> may want to use the same gesture for the television, or for that matter for the thermostat or light switch, in any room at home. This implies omnipresent audio and video collection within the home.

All of these audio, video, and sensor data will be generated within the supposed sanctuary of the home. But they are no more likely to stay in the home than the “papers and effects” already discussed. Electronic devices in the home already invisibly communicate to the outside world via multiple separate infrastructures: The cable industry’s hardwired connection to the home provides multiple types of two-way communication, including broadband Internet. Wireline phone is still used by some home-intrusion alarms and satellite TV receivers, and as the physical layer for DSL broadband subscribers. Some home devices use the cell-phone wireless infrastructure. Many others piggyback on the home Wi-Fi network that is increasingly a necessity of modern life. Today’s smart home-entertainment system knows what a person records on a DVR, what she actually watches, and when she watches it. Like personal financial records in 2000, this information today is in part localized inside the home, on the hard drive inside the DVR. As with financial information today, however, it is on track to move into the cloud. Today, Netflix or Amazon can offer entertainment suggestions based on customers’ past key-click streams and viewing history on their platforms. Tomorrow, even better suggestions may be enabled by interpreting their minute-by-minute facial expressions as seen by the gesture-reading camera in the television.

These collections of data are benign, in the sense that they are necessary for products and services that consumers will knowingly demand. Their challenges to privacy arise both from the fact that their analog sensors necessarily collect more information than is minimally necessary for their function (see Section 3.1.2), and also because their data practically cry out for secondary uses ranging from innovative new products to marketing bonanzas to criminal exploits. As in many other kinds of big data, there is ambiguity as to data ownership, data rights, and allowed data use. Computer-vision software is likely already able to read the brand labels on products in its field of view – this is a much easier technology than facial recognition. If the camera in your television knows what brand of beer you are drinking while watching a football game, and knows whether you opened the bottle before or after the beer ad, who (if anyone) is allowed to sell this information to the beer company, or to its competitors? Is the camera allowed to read brand names when the television set is supposedly off? Can it watch for magazines or political leaflets? If the RFID tag sensor in your refrigerator usefully detects out-of-date food, can it also report your brand choices to vendors? Is this creepy and strange, or a consumer financial benefit when every supermarket can offer you relevant coupons?<sup>50</sup> Or (the dilemma of

<sup>47</sup> Reuters, “Apple acquires Israeli 3D chip developer PrimeSense,” November 25, 2013.

<sup>48</sup> <http://www.reuters.com/article/2013/11/25/us-primesense-offer-apple-idUSBRE9AO04C20131125>

<sup>49</sup> *Id.*

<sup>50</sup> Google, “Glass gestures,” <https://support.google.com/glass/answer/3064184?hl=en>

<sup>50</sup> Tene, Omer, and Jules Polonetsky, “A Theory of Creepy: Technology, Privacy and Shifting Social Norms,” *Yale Journal of Law and Technology* 16:59, 2013, pp. 59-100.

differential pricing<sup>51</sup>) is it any different if the data are used to offer *others* a better deal while *you* pay full price because your brand loyalty is known to be strong?

About one-third of Americans rent, rather than own, their residences. This number may increase with time as a result of long-term effects of the 2007 financial crisis, as well as aging of the U.S. population. Today and foreseeably, renters are less affluent, on average, than homeowners. The law demarcates a fine line between the property rights of landlords and the privacy rights of tenants. Landlords have the right to enter their property under various conditions, generally including where the tenant has violated health or safety codes, or to make repairs. As more data are collected within the home, the rights of tenant and landlord may need new adjustment. If environmental monitors are fixtures of the landlord's property, does she have an unconditional right to their data? Can she sell those data? If the lease so provides, can she evict the tenant if the monitor repeatedly detects cigarette smoke, or a camera sensor is able to distinguish a prohibited pet?

If a third party offers facial recognition services for landlords (no doubt with all kinds of cryptographic safeguards!), can the landlord use these data to enforce lease provisions against subletting or additional residents? Can she require such monitoring as a condition of the lease? What if the landlord's cameras are outside the doors, but keep track of everyone who enters or leaves her property? How is this different from the case of a security camera across the street that is owned by the local police?

## 2.4 Tradeoffs among privacy, security, and convenience

Notions of privacy change generationally. One sees today marked differences between the younger generation of "digital natives" and their parents or grandparents. In turn, the children of today's digital natives will likely have still different attitudes about the flow of their personal information. Raised in a world with digital assistants who know everything about them, and (one may hope) with wise policies in force to govern use of the data, future generations may see little threat in scenarios that individuals today would find threatening, if not Orwellian. PCAST's final scenario, perhaps at the outer limit of its ability to prognosticate, is constructed to illustrate this point.

Taylor Rodriguez prepares for a short business trip. She packed a bag the night before and put it outside the front door of her home for pickup. No worries that it will be stolen: The camera on the streetlight was watching it; and, in any case, almost every item in it has a tiny RFID tag. Any would-be thief would be tracked and arrested within minutes. Nor is there any need to give explicit instructions to the delivery company, because the cloud knows Taylor's itinerary and plans; the bag is picked up overnight and will be in Taylor's destination hotel room by the time of her arrival.

Taylor finishes breakfast and steps out the front door. Knowing the schedule, the cloud has provided a self-driving car, waiting at the curb. At the airport, Taylor walks directly to the gate – no need to go through any security. Nor are there any formalities at the gate: A twenty-minute "open door" interval is provided for passengers to stroll onto the plane and take their seats (which each sees individually highlighted in his or her wearable optical device). There are no boarding passes and no organized lines. Why bother, when Taylor's identity (as for everyone else who enters the airport) has been tracked and is known absolutely? When her known information emanations (phone, RFID tags in clothes, facial recognition, gait, emotional state) are known to the cloud, vetted, and essentially unforgeable? When, in the unlikely event that Taylor has become deranged and dangerous, many detectable signs would already have been tracked, detected, and acted on?

---

<sup>51</sup> See references at footnote 30.

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

Indeed, everything that Taylor carries has been screened far more effectively than any rushed airport search today. Friendly cameras in every LED lighting fixture in Taylor's house have watched her dress and pack, as they do every day. Normally these data would be used only by Taylor's personal digital assistants, perhaps to offer reminders or fashion advice. As a condition of using the airport transit system, however, Taylor has authorized the use of the data for ensuring airport security and public safety.

Taylor's world seems creepy to us. Taylor has accepted a different balance among the public goods of convenience, privacy, and security than would most people today. Taylor acts in the unconscious belief (whether justified or not, depending on the nature and effectiveness of policies in force) that the cloud and its robotic servants are trustworthy in matters of personal privacy. In such a world, major improvements in the convenience and security of everyday life become possible.



### 3. Collection, Analytics, and Supporting Infrastructure

Big data is big in two different senses. It is big in the quantity and variety of data that are available to be processed. And, it is big in the scale of analysis (“analytics”) that can be applied to those data, ultimately to make inferences. Both kinds of “big” depend on the existence of a massive and widely available computational infrastructure, one that is increasingly being provided by cloud services. This chapter expands on these basic concepts.

#### 3.1 Electronic sources of personal data

Since early in the computer age, public and private entities have been assembling digital information about people. Databases of personal information were created during the days of “batch processing.”<sup>52</sup> Indeed, early descriptions of database technology often talk about personnel records used for payroll applications. As computing power increased, more and more business applications moved to digital form. There now are digital telephone-call records, credit-card transaction records, bank-account records, email repositories, and so on. As interactive computing has advanced, individuals have entered more and more data about themselves, both for self-identification to an online service and for productivity tools such as financial-management systems.

These digital data are normally accompanied by “metadata” or ancillary data that explain the layout and meaning of the data they describe. Databases have schemas and email has headers,<sup>53</sup> as do network packets.<sup>54</sup> As data sets become more complex, so do the attached metadata. Included in the data or metadata may be identifying information such as account numbers, login names, and passwords. There is no reason to believe that metadata raise fewer privacy concerns than the data they describe.

In recent times, the kinds of electronic data available about people have increased substantially, in part because of the emergence of social media and in part because of the growth in mobile devices, surveillance devices, and a diversity of networked sensors. Today, although they may not be aware of it, individuals constantly emit into the environment information whose use or misuse may be a source of privacy concerns. Physically, these information emanations are of two types, which can be called “born digital” or “born analog.”

##### 3.1.1 “Born digital” data

When information is “born digital,” it is created, by us or by a computer surrogate, specifically for digital use – that is, for use by a computer or data-processing system. Examples of data that are born digital include:

- email and text messaging
- input via mouse-clicks, taps, swipes, or keystrokes on a phone, tablet, computer, or video game; that is, data that people intentionally enter into a device

<sup>52</sup> Such databases endure and form the basis of continuing concern among privacy advocates.

<sup>53</sup> Schemas are formal definitions of the configuration of a database: its tables, relations, and indices. Headers are the sometimes-invisible prefaces to email messages that contain information about the sending and destination addresses and sometimes the routing of the path between them.

<sup>54</sup> In the Internet and similar networks, information is broken up into chunks called packets, which may travel independently and depend on metadata to be reassembled properly at the destination of the transmission.

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

- GPS location data
- metadata associated with phone calls: the numbers dialed from or to, the time and duration of calls
- data associated with most commercial transactions: credit-card swipes, bar-code reads, reads of RFID tags (as used for anti-theft and inventory control)
- data associated with portal access (key card or ID badge reads) and toll-road access (remote reads of RFID tags)
- metadata that our mobile devices use to stay connected to the network, including device location and status
- increasingly, data from cars, televisions, appliances: the “Internet of Things”

Consumer-tracking data provide an example of born-digital data that has become economically important. It is generally possible for companies to aggregate large amounts of data and then use those data for marketing, advertising, or many other activities. The traditional mechanism has been to use cookies, small data files that a browser can leave on a user’s computer (pioneered by Netscape two decades ago). The technique is to leave a cookie when a user first visits a site and then be able to correlate that visit with a subsequent event. This information is very valuable to retailers and forms the basis of many of the advertising businesses of the last decade. There has been a variety of proposals to regulate such tracking,<sup>55</sup> and many countries require opt-in permission before this tracking is done. Cookies involve relatively simple pieces of information that proponents represent as unlikely to be abused. Although not always aware of the process, people accept such tracking in return for a free or subsidized service.<sup>56</sup> At the same time, cookie-free alternatives are sometimes available.<sup>57</sup> Even without cookies, so-called “fingerprinting” techniques can often identify a user’s computer or mobile device uniquely by the information that it exposes publicly, such as the size of its screen, its installed fonts, and other features.<sup>58</sup> Most technologists believe that applications will move away from cookies, that cookies are too simple an idea, and that there are better analytics coming and better approaches being invented. The economic incentives for consumer tracking will remain, however, and big data will allow for more precise responses.

Tracking is also the enabling technology of some more nefarious uses. Unfortunately, many social networking apps begin by taking a person’s contact list and spamming all the recipients with advertising for the app. This technique is often abused, especially by small start-ups who may assess the value gained by reaching new customers as being greater than the value lost to their reputation for honoring privacy.

---

<sup>55</sup> Federal Trade Commission, “FTC Staff Revises Online Behavioral Advertising Principles,” Press Release, February 12, 2009. <http://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles>

<sup>56</sup> (1) Cf. *The Wall Street Journal*’s “What they know” series (<http://online.wsj.com/public/page/what-they-know-digital-privacy.html>). (2) Turov, Joseph, *The Daily You: How the Advertising Industry is Defining your Identity and Your Worth*, Yale University Press, 2012. <http://yalepress.yale.edu/book.asp?isbn=9780300165012>

<sup>57</sup> DuckDuckGo is a non-tracking search engine that, while perhaps yielding fewer results than leading search engines, is used by those looking for less tracking. See: <https://duckduckgo.com/>

<sup>58</sup> (1) Tanner, Adam, “The Web Cookie Is Dying. Here’s The Creepier Technology That Comes Next,” *Forbes*, June 17, 2013. <http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/> (2) Acar, G. et al., “FPDetective: Dusting the Web for Fingerprints,” 2013. <http://www.cosic.esat.kuleuven.be/publications/article-2334.pdf>

All information that is born digital shares certain characteristics. It is created in identifiable units for particular purposes. These units are in most cases “data packets” of one or another standard type. Since they are created by intent, the information that they contain is usually limited, for reasons of efficiency and good engineering design, to support the immediate purpose for which they are collected.

When data are born digital, privacy concerns can arise in two different modes, one obvious (“over-collection”), the other more recent and subtle (“data fusion”). Over-collection occurs when an engineering design intentionally, and sometimes clandestinely, collects information unrelated to its stated purpose. While your smartphone could easily photograph and transmit to a third party your facial expression as you type every keystroke of a text message, or could capture all keystrokes, thereby recording text that you had deleted, these would be inefficient and unreasonable software design choices for the default text-messaging app. In that context they would be instances of over-collection.

A recent example of over-collection was the *Brightest Flashlight Free* phone app, downloaded by more than 50 million users, which passed back to its vendor its location every time the flashlight was used. Not only is location information unnecessary for the illumination function of a flashlight, but it also discloses personal information that the user might wish to keep private. The Federal Trade Commission issued a complaint because the fine print on the notice-and-consent screen (see Section 4.3) had neglected to disclose that location information, whose collection was disclosed, would be sold to third parties, such as advertisers.<sup>59,60</sup> One sees in this example the limitations of the notice-and-consent framework: A more detailed initial fine-print disclosure by *Brightest Flashlight Free*, which almost no one would have actually read, would likely have forestalled any FTC action without much affecting the number of downloads.

In contrast to over-collection, data fusion occurs when data from different sources are brought into contact and new, often unexpected, phenomena emerge (see Section 3.1). Individually, each data source may have been designed for a specific, limited purpose. But when multiple sources are processed by techniques of modern statistical data mining, pattern recognition, and the combining of records from diverse sources by virtue of common identifying data, new meanings can be found. In particular, data fusion frequently results in the identification of individual people (that is, the association of events with unique personal identities), the creation of data-rich profiles of an individual, and the tracking of an individual’s activities over days, months, or years.

By definition, the privacy challenges from data fusion do not lie in the individual data streams, each of whose collection, real-time processing, and retention may be wholly necessary and appropriate for its overt, immediate purpose. Rather, the privacy challenges are emergent properties of our increasing ability to bring into analytical juxtaposition large, diverse data sets and to process them with new kinds of mathematical algorithms.

---

<sup>59</sup> Federal Trade Commission, “Android Flashlight App Developer Settles FTC Charges It Deceived Consumers,” *Press Release*, December 5, 2013. <http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived>

<sup>60</sup> (1) FTC File No. 132-3087 Decision and order. <http://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf> (2) “FTC Approves Final Order Settling Charges Against Flashlight App Creator.” <http://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app>

### 3.1.2 Data from sensors

Turn now to the second broad class of information emanations. One can say that information is “born analog” when it arises from the characteristics of the physical world. Such information does not become accessible electronically until it impinges on a “sensor,” an engineered device that observes physical effects and converts them to digital form. The most common sensors are cameras, including video, which sense visible electromagnetic radiation; and microphones, which sense sound and vibration. There are many other kinds of sensors, however. Today, cell phones routinely contain not only cameras, microphones, and radios but also analog sensors for magnetic fields (3-D compass) and motion (acceleration). Other kinds of sensors include those for thermal infrared (IR) radiation; air quality, including the identification of chemical pollutants; barometric pressure (and altitude); low-level gamma radiation; and many other phenomena.

Examples of born-analog data providing personal information and in use today include:

- the voice and/or video content of a phone call – born analog but immediately converted to digital by the phone’s microphone and camera
- personal health data such as heartbeat, respiration, and gait, as sensed by special-purpose devices (Fitbit has been a leading provider<sup>61</sup>) or cell-phone apps
- cameras/sensors in televisions and video games that interpret gestures by the user
- video from security surveillance cameras, mobile phones, or overhead drones
- imaging infrared video that can see in what people perceive as total darkness (and also see evanescent traces of past events, so-called heat scars)
- microphone networks in cities, used to detect and locate gunshots and for public safety
- cameras/microphones in classrooms and other meeting rooms
- ultrasonic motion detectors
- medical imaging, CT, and MRI scans, ultrasonic imaging
- opportunistically collected chemical or biological samples, notably trace DNA (today requiring slow, off-line analysis, but foreseeably more nimble)
- synthetic aperture radar (SAR), which can image through clouds and, under some conditions, see inside of non-metallic structures
- unintended radiofrequency emissions from electrical and electronic devices

When data are born analog, they are likely to contain more information than the minimum necessary for their immediate purpose, for several valid reasons. One is that the desired information (“signal”) must be sensed in the presence of unwanted extraneous information (“noise”). The technologies typically work by sensing the environment (“signal plus noise”) with high precision, so that mathematical techniques can then be applied that will separate the two even in the worst anticipated case when the signal is smallest or the noise is largest.

Another reason is technological convergence. For example, as the cameras in cell phones become smaller and cheaper, the use of identical components in other products becomes a favored design choice, even when full images are not needed. Where a big-screen television today has separate sensors for its IR remote control, room brightness, and motion detection (a feature that turns off the picture when no one is in the room), plus a true video camera in the add-on game console, tomorrow’s model may integrate all of these functions in a single, cheap, high-resolution, IR-sensitive camera, a few millimeters in size.

---

<sup>61</sup> See: <http://www.fitbit.com/>

In addition to the information available from digital and analog sources consciously intended to provide information about people, inadvertent disclosure abounds from the emerging “Internet of Things,” an amalgamation of sensors whose primary purpose is enhanced by “smart” network-connected computational capabilities. Examples include “smart” thermostats that detect human presence and adjust air temperatures accordingly, “smart” automobile-ignition systems, and locking systems that are biometrically triggered.

The privacy challenges of born-analog data are somewhat different from those of born-digital data. Where over-collection (as was defined above) is an irrational design choice for the principled digital designer – and therefore an identifiable red flag for privacy issues – over-collection in the analog domain can be a robust and economical design choice. A consequence is that born-analog data will often contain information that was not originally expected. Unexpected information could in many cases lead to unanticipated beneficial products and services, but it could also give opportunities for unanticipated misuse.

As a concrete example, one might consider three key parameters of video imaging: resolution (how many pixels in the image), contrast ratio (how well can the image see into dark regions), and photometric precision (how accurate is the image in brightness and color). All three parameters have improved by orders of magnitude and are likely to keep improving. Today, with special cameras, one can image a cityscape from a high rooftop and see clearly into every facing house and apartment window within several miles.<sup>62</sup> Or, already mentioned, the ability exists to sense remotely the pulse of an individual, giving information on health status and emotional state.<sup>63</sup>

It is foreseeable, perhaps inevitable, that these capabilities will be present in every cell phone and security-surveillance camera, or every wearable computer device. (Imagine the process of negotiating the price for a car, or negotiating an international trade agreement, when every participant’s Google Glass (or security camera or TV camera) is able to monitor and interpret the autonomic physiological state of every other participant, in real time.) It is unforeseeable what other unexpected information also lies in signals from the same sensors.

Once they enter the digital world, born-analog data can be fused and mined along with born-digital data. For example, facial-recognition algorithms, which might be error-prone in isolation, may yield nearly perfect identity tracking when they can be combined with born-digital data from cell phones (including unintended emanations), point-of-sale transactions, RFID tags, and so forth; and also with other born-analog data such as vehicle tracking (e.g., from overhead drones) and automated license-plate reading. Biometric data can provide identity information that enhances the profile of an individual even more, and data on behavior (as from social networks) are being used to analyze attitudes or emotions (“sentiment analysis,” for individuals or groups<sup>64</sup>). In short, more and more information can be captured and put in a quantified format so it can be tabulated and analyzed.<sup>65</sup>

<sup>62</sup> Koonin, Steven E., Gregory Dobler and Jonathan S. Wurtele, “Urban Physics,” *American Physical Society News*, March, 2014. <http://www.aps.org/publications/apsnews/201403/urban.cfm>

<sup>63</sup> Durand, Fredo, et al., “MIT Computer Program Reveals Invisible Motion in Video,” *The New York Times*, video, February 27, 2013. <https://www.youtube.com/watch?v=3rWvcBEHn3s>

<sup>64</sup> Feldman, Ronen, “Techniques and Applications for Sentiment Analysis,” *Communications of the ACM*, 56:4, pp. 82-89.

<sup>65</sup> Mayer-Schönberger, Viktor and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston, NY: Houghton Mifflin Harcourt, 2013.



### 3.2 Big data analytics

Analytics is what makes big data come alive. Without analytics, big datasets could be stored, and they could be retrieved, wholly or selectively. But what comes out would be exactly what went in. Analytics, comprising a number of different computational technologies, is what fuels the big-data revolution.<sup>66</sup> Analytics is what creates the new value in big datasets, vastly more than the sum of the values of the parts.<sup>67</sup>

#### 3.2.1 Data mining

Data-mining, sometimes loosely equated to analytics but actually only a subset of it, refers to a computational process that discovers patterns in large data sets. It is a convergence of many fields of academic research in both applied mathematics and computer science, including statistics, databases, artificial intelligence, and machine learning. Like other technologies, advances in data mining have a research and development stage, in which new algorithms and computer programs are developed, and they have subsequent phases of commercialization and application.

Data mining algorithms can be trained to find patterns either by supervised learning, so-called because the algorithm is seeded with manually curated examples of the pattern to be recognized, or by unsupervised learning, where the algorithm tries to find related pieces of data without prior seeding. A recent success of unsupervised-learning algorithms was a program that, searching millions of images on the web, figured out on its own that “cat” was a much-posted category.<sup>68</sup>

The desired output of data mining can take several forms, each with its own specialized algorithms.<sup>69</sup>

- Classification algorithms attempt to assign objects or events to known categories. For example, a hospital might want to classify discharged patients as high, medium, or low risk for readmission.
- Clustering algorithms group objects or events into categories by similarity, as in the “cat” example above.
- Regression algorithms (also called numerical prediction algorithms) try to predict numerical quantities. For example, a bank may want to predict, from the details in a loan application, the probability of a default.
- Association techniques try to find relationships between items in their data set. Amazon’s suggested products and Netflix’s suggested movies are examples.
- Anomaly-detection algorithms look for untypical examples within a data set, for example, detecting fraudulent transactions on a credit-card account.
- Summarization techniques attempt to find and present salient features in data. Examples include both simple statistical summaries (e.g., average student test scores by school and teacher), and higher-level analysis (e.g., a list of key facts about an individual as gleaned from all web postings that mention her).

<sup>66</sup> National Research Council, *Frontiers in Massive Data Analysis*, National Academies Press, 2013.

<sup>67</sup> (1) Thill, Brent and Nicole Hayashi, *Big Data = Big Disruption: One of the Most Transformative IT Trends Over the Next Decade*, UBS Securities LLC, October 2013. (2) McKinsey Global Institute, Center for Government, and Business Technology Office, *Open data: Unlocking innovation and performance with liquid information*, McKinsey & Company, October 2013.

<sup>68</sup> Le, Q.V. et al., “Building High-level Features Using Large Scale Unsupervised Learning,”

[http://static.googleusercontent.com/media/research.google.com/en/us/archive/unsupervised\\_icml2012.pdf](http://static.googleusercontent.com/media/research.google.com/en/us/archive/unsupervised_icml2012.pdf)

<sup>69</sup> Bramer, M., “Principles of Data Mining,” *Springer*, 2013.

Data mining is sometimes confused with machine learning, the latter a broad subfield of computer science in academic and industrial research.<sup>70</sup> Data mining makes use of machine learning, as well as other disciplines, while machine learning has applications to fields other than data mining, for example, robotics.

There are limitations, both practical and theoretical, to what data mining can accomplish, as well as limits to how accurate it can be. It may reveal patterns and relationships, but it usually cannot tell the user the value or significance of these patterns. For example, supervised learning based on the characteristics of known terrorists might find similar persons, but they might or might not be terrorists; and it would miss different classes of terrorists who don't fit the profile.

Data mining can identify relationships between behaviors and/or variables, but these relationships do not always indicate causality. If people who live under high-voltage power lines have higher morbidity, it might mean that power lines are a hazard to public health; or it might mean that people who live under power lines tend to be poor and have inadequate access to health care. The policy implications are quite different. While so-called confounding variables (in this example, income) can be corrected for when they are known and understood, there is no sure way to know whether all of them have been identified. Imputing true causality in big data is a research field in its infancy.<sup>71</sup>

Many data analyses yield correlations that might or might not reflect causation. Some data analyses develop imperfect information, either because of limitations of the algorithms, or by the use of biased sampling. Indiscriminate use of these analyses may cause discrimination against individuals or a lack of fairness because of incorrect association with a particular group.<sup>72</sup> In using data analyses, particular care must be taken to protect the privacy of children and other protected groups.

Real-world data are incomplete and noisy. These data-quality issues lower the performance of data-mining algorithms and obscure outputs. When economics allow, careful screening and preparation of the input data can improve the quality of results, but this data preparation is often labor intensive and expensive. Users, especially in the commercial sector, must trade off cost and accuracy, sometimes with negative consequences for the individual represented in the data. Additionally, real-world data can contain extreme events or outliers. Outliers may be real events that, by chance, are overrepresented in the data; or they may be the result of data-entry or data-transmission errors. In both cases they can skew the model and degrade performance. The study of outliers is an important research area of statistics.

### 3.2.2 Data fusion and information integration

Data fusion is the merging of multiple heterogeneous datasets into one homogeneous representation so that they can be better processed for data mining and management. Data fusion is used in a number of technical domains such as sensor networks, video/image processing, robotics and intelligent systems, and elsewhere.

<sup>70</sup> Mitchell, Tom M., "The Discipline of Machine Learning," Technical Report CMU-ML-06-108, Carnegie Mellon University, July 2006.

<sup>71</sup> DARPA, for example, has a project involving machine learning and other technologies to build medical causal models from analysis of cancer literature, leveraging the greater capacity of a computer than a person to process information from a large number of sources. See description at [http://www.darpa.mil/Our\\_Work/I2O/Programs/Big\\_Mechanism.aspx](http://www.darpa.mil/Our_Work/I2O/Programs/Big_Mechanism.aspx)

<sup>72</sup> "Data mining breaks the basic intuition that identity is the greatest source of potential harm because it substitutes inference for identifying information as a bridge to get at additional facts." Barocas, Solon and Helen Nissenbaum, "Big Data's End Run Around Anonymity and Consent," Chapter II, in Lane, Julia, et al., *Privacy, Big Data, and the Public Good*, Cambridge University Press, 2014.

Data integration is differentiated from data fusion in that integration more broadly combines data sets and retains the larger set of information. In data fusion, there is usually a reduction or replacement technique. Data fusion is facilitated by data interoperability, the ability for two systems to communicate and exchange data.

Data fusion and data integration are key techniques for business intelligence. Retailers are integrating their online, in-store, and catalog sales databases to create more complete pictures of their customers. Williams-Sonoma, for example, has integrated customer databases with information on 60 million households. Variables including household income, housing values, and number of children are tracked. It is claimed that targeted emails based on this information yield ten to 18 times the response rate of emails that are not targeted.<sup>73</sup> This is a simple illustration of how more information can lead to better inferences. Techniques that can help to preserve privacy are emerging.<sup>74</sup>

There is a great amount of interest today in multi-sensor data fusion.<sup>75</sup> The biggest technical challenges being tackled today, generally through development of new and better algorithms, relate to data precision/resolution, outliers and spurious data, conflicting data, modality (both heterogeneous and homogeneous data) and dimensionality, data correlation, data alignment, association within data, centralized vs. decentralized processing, operational timing, and the ability to handle dynamic vs. static phenomena. Privacy concerns may arise from sensor fidelity and precision as well as correlation of data from multiple sensors. A single sensor's output might not be sensitive, but the combination from two or more may raise privacy concerns.

### 3.2.3 Image and speech recognition

Image- and speech-recognition technologies are able to extract information, in some limited cases approaching human understanding, from massive corpuses of still images, videos, and recorded or broadcast speech.

Urban-scene extraction can be accomplished using a variety of data sources from photos and videos to ground based LIDAR (a remote-sensing technique using lasers).<sup>76</sup> In the government sector, city models are becoming vital for urban planning and visualization. They are equally important for a broad range of academic disciplines including history, archeology, geography, and computer-graphics research. Digital city models are also central to popular consumer mapping and visualization applications such as Google Earth and Bing Maps, as well as GPS-enabled navigation systems.<sup>77</sup> Scene extraction is an example of the inadvertent capture of personal information and can be used for data fusion that reveals personal information.

Facial-recognition technologies are beginning to be practical in commercial and law-enforcement applications.<sup>78</sup> They are able to acquire, normalize, and recognize moving faces in dynamic scenes. Real-time video surveillance with single-camera systems (and some with multi-camera systems, which can both recognize objects and analyze activity) has a wide variety of applications in both public and private environments, such as homeland

<sup>73</sup> Manyika, J. et al., "Big Data: The next frontier for innovation, competition, and productivity," *McKinsey Global Institute*, 2011.

<sup>74</sup> Navarro-Arriba, G. and V. Torra, "Information fusion in data privacy: A survey," *Information Fusion*, 13:4, 2012, pp. 235-244.

<sup>75</sup> Khaleghi, B. et al., "Multisensor data fusion: A review of the state-of-the-art," *Information Fusion*, 14:1, 2013, pp. 28-44.

<sup>76</sup> Lam, J., et al., "Urban scene extraction from mobile ground based lidar data," *Proceedings of 3DPVT*, 2010.

<sup>77</sup> Agarwal, S., et al., "Building Rome in a day," *Communications of the ACM*, 54:10, 2011, pp. 105-112.

<sup>78</sup> Workshop on Frontiers in Image and Video Analysis, National Science Foundation, Federal Bureau of Investigation, Defense Advanced Research Projects Agency, and University of Maryland Institute for Advanced Computer Studies, January 28-29, 2014. <http://www.umiacs.umd.edu/conferences/fiva/>

security, crime prevention, traffic control, accident prediction and detection, and monitoring patients, the elderly, and children at home.<sup>79</sup> Depending on the application, use of video surveillance is at varying levels of deployment.<sup>80</sup>

Additional capabilities of image recognition include

- Video summarization and scene-change detection (that is, picking the small number of images that summarize a period of time)
- Precise geolocation in imagery from satellites or drones
- Image-based biometrics
- Human-in-the-loop surveillance systems
- Re-identification of persons and vehicles, that is, tracking the same person or vehicle as it moves from sensor to sensor
- Human-activity recognition of various kinds
- Semantic summarization (that is, converting pictures into text summaries)

Although systems are expected to become able to track objects across camera views and detect unusual activities in a large area by combining information from multiple sources, re-identification of objects remains hard to do (a challenge for inter-camera tracking), as is video surveillance in crowded environments.

Although the data they use are often captured in public areas, scene-extraction technologies like Google Street View have triggered privacy concerns. Photos captured for use in Street View may contain sensitive information about people who are unaware they are being observed and photographed.<sup>81</sup>

Social-media data can be used as an input source for scene extraction techniques. When these data are posted, however, users are unlikely to know that their data would be used in these aggregated ways and that their social media information (although public) might appear synthesized in new forms.<sup>82</sup>

Automated speech recognition has existed since at least the 1950s,<sup>83</sup> but recent developments over the last 10 years have allowed for novel new capabilities. Spoken text (e.g., news broadcasters reading part of a document) can today be recognized with accuracy higher than 95 percent using state-of-the-art techniques. Spontaneous speech is much harder to recognize accurately. In recent years there has been a dramatic increase in the corpuses of spontaneous speech data available to researchers, which has allowed for improved accuracy.

---

<sup>79</sup> For example, Newark Airport recently installed a system of 171 LED lights (from Sensity <http://www.sensity.com/>) that contain special chips to connect to sensors and cameras over a wireless system. These systems allow for advanced automatic lighting to improve security in places like parking garages, and in doing so capture a large range of information.

<sup>80</sup> This was discussed at the workshop cited in footnote 78.

<sup>81</sup> Such concerns are likely to grow as commercial satellite imagery systems such as Skybox (<http://skybox.com/>) provide the basis for more services.

<sup>82</sup> Billitteri, Thomas J., et al. "Social Media Explosion: Do social networking sites threaten privacy rights?" *CQ Researcher*, January 25, 2013, 23:84-104.

<sup>83</sup> Juang, B.H. and Lawrence R. Rabiner, "Automated Speech Recognition – A Brief History of the Technology Development," October 8, 2004. [http://www.ece.ucsb.edu/Faculty/Rabiner/ece259/Reprints/354\\_LALI-ASRHistory-final-10-8.pdf](http://www.ece.ucsb.edu/Faculty/Rabiner/ece259/Reprints/354_LALI-ASRHistory-final-10-8.pdf)

Over the next few years speech-recognition interfaces will be in many more places. For example, multiple companies are exploring speech recognition to control televisions and cars, to find a show on TV, or to schedule a DVR recording. Researchers at Nuance say they are actively planning how speech technology would have to be designed to be available on wearable computers.<sup>84</sup> Google has already implemented some of this basic functionality in its Google Glass product, and Microsoft's Xbox One system already integrates machine vision and multi-microphone audio input for controlling system functions.

### 3.2.4 Social-network analysis

Social-network analysis refers to the extraction of information from a variety of interconnecting units under the assumption that their relationships are important and that the units do not behave autonomously.<sup>85</sup> Social networks often emerge in an online context. The most obvious examples are dedicated online social media platforms, such as Facebook, LinkedIn and Twitter, which provide new access to social interaction by allowing users to connect directly with each other over the Internet to communicate and share information. Offline human social networks may also leave analyzable digital traces, such as in phone-call metadata records that record which phones have exchanged calls or texts, and for how long. Analysis of social networks is increasingly enabled by the rising collection of digital data that links people together, especially when it is correlated to other data or metadata about the individual.<sup>86</sup> Tools for such analysis are being developed and made available,<sup>87</sup> motivated in part by the growing amount of social network content accessible through open application-programming interfaces to online social-media platforms. This sort of analysis is an active arena for research.

Social-network analysis complements analysis of conventional databases, and some of the techniques used (e.g., clustering in association networks) can be used in either context. Social-network analysis can be more powerful because of the easy association of diverse kinds of information (i.e., considerable data fusion is possible). It lends itself to visualization of the results, which aids in interpreting the results of the analysis. It can be used to learn about people through their association with others, in a context of people's tendency to associate with others who are have some similarities to themselves.<sup>88</sup>

Social-network analysis is yielding results that may surprise people. In particular, unique identification of an individual is easier than from database analysis alone. Moreover, it is achieved through more diverse kinds of

<sup>84</sup> "Where Speech Recognition is Going," *Technology Review*, May 29, 2012. <http://www.kurzweilai.net/where-speech-recognition-is-going>

<sup>85</sup> Wasserman, S. "Social network analysis: Methods and applications," *Cambridge University Press*, 8, 1994.

<sup>86</sup> See, for example: (1) Backstrom, Lars, et al., "Inferring Social Ties from Geographic Coincidences," *Proceedings of the National Academy of Sciences*, 2010. (2) Backstrom, Lars, et al., "Wherefore Art Though R3579X? Anonymized Social Networks, Hidden Patterns, and Structural Steganography," *International World Wide Web Conference 2007*, Alberta, Canada, May 12, 2007.

<sup>87</sup> A variety of tools exist for managing, analyzing, visualizing and manipulating network (graph) datasets, such as Allegrograph, GraphVis, R, visone and Wolfram Alpha. Some, such as Cytoscape, Gephi and Netviz are open source.

<sup>88</sup> (1) Geetoor, L. and E. Zheleva, "Preserving the privacy of sensitive relationships in graph data," *Privacy, security, and trust in KDD*, 153-171, 2008. (2) Mislove, A., et al., "An analysis of social-based network Sybil defenses," *ACM SIGCOMM Computer Communication Review*, 2011. (3) Backstrom, Lars, et al., "Find Me If You Can: Improving Geographic Prediction with Social and Spatial Proximity," *Proceedings of the 19th international conference on World Wide Web*, 2010. (4) Backstrom, L. and J. Kleinberg, "Romantic Partnerships and the Dispersion of Social Ties: A Network Analysis of Relationship Status on Facebook," *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*, 2014.

data than many people may understand, contributing to the erosion of anonymity.<sup>89</sup> The structure of an individual's network is unique and itself serves as an identifier; co-occurrence in time and space is a significant means of identification; and, as discussed elsewhere in this report, different kinds of data can be combined to foster identification.<sup>90</sup>

Social-network analysis is used in criminal forensic investigations to understand the links, means, and motives of those who may have committed crimes. In particular, social-network analysis has been used to better understand covert terrorist networks, whose dynamics may be different from those of overt networks.<sup>91</sup>

In the realm of commerce, it is well-understood that what a person's friends like or buy can influence what he or she might buy. For example, in 2010, it was reported that having one iPhone-owning friend makes a person three times more likely to own an iPhone than otherwise. A person with two iPhone-owning friends was five times more likely to have one.<sup>92</sup> Such correlations emerge in social-network analysis and can be used to help predict product trends, tailor marketing campaigns towards products an individual may be more likely to want, and target customers (said to have higher "network value") with a central role (and a large amount of influence) in a social network.<sup>93</sup>

Because disease is commonly spread via direct contact between individuals (humans or animals), understanding social networks through whatever proxies are available can suggest possible direct contacts and thereby assist in monitoring and stemming the outbreak of disease.

A recent study by researchers at Facebook analyzed the relationship between geographic location of individual users and that of their friends. From this analysis, they were able to create an algorithm to predict the location of an individual user based upon the locations of a small number of friends in their network, with higher accuracy than simply looking at the user's IP address.<sup>94</sup>

There are many commercial "social listening" services, such as Radian6/Salesforce Cloud, Collective Intellect, Lithium, and others, that mine data from social-networking feeds for use in business intelligence.<sup>95</sup> Coupled

---

<sup>89</sup> (1) Narayanan, A. and V. Shmatikov, "De-anonymizing social networks," *30th IEEE Symposium on Security and Privacy*, 173-187, 2009. (2) Crandall, David J., et al., "Inferring social ties from geographic coincidences," *Proceedings of the National Academy of Sciences*, 107:52, 2010. (3) Backstrom, L. C. Dwork and J. Kleinberg, "Wherefore Art Thou R3579X? Anonymized Social Networks, Hidden Patterns, and Structural Steganography," *Proceedings of the 16th Intl. World Wide Web Conference*, 2007. (4) Saramäki, Jari, et al., "Persistence of social signatures in human communication," *Proceedings of the National Academy of Sciences*, 111.3:942-947, 2014.

<sup>90</sup> Fienberg, S.E., "Is the Privacy of Network Data an Oxymoron?" *Journal of Privacy and Confidentiality*, 4:2, 2013.

<sup>91</sup> Krebs, V.E., "Mapping networks of terrorist cells," *Connections*, 24.3:43-52, 2002.

<sup>92</sup> Sundsøy, P. R., et al., "Product adoption networks and their growth in a large mobile phone network," *Advances in Social Networks Analysis and Mining (ASONAM)*, 2010.

<sup>93</sup> Hodgson, Bob, "A Vital New Marketing Metric: The Network Value of a Customer," *Predictive Marketing: Optimize Your ROI With Analytics*. <http://predictive-marketing.com/index.php/a-vital-new-marketing-metric-the-network-value-of-a-customer/>

<sup>94</sup> Backstrom, Lars et al, "Find me if you can: improving geographical prediction with social and spatial proximity," *Proceedings of the 19th international conference on World Wide Web*, 2010.

<sup>95</sup> "Top 20 social media monitoring vendors for business," *Socialmedia.biz*, <http://socialmedia.biz/2011/01/12/top-20-social-media-monitoring-vendors-for-business/>

with social-network analysis, this information can be used to evaluate changing influences and the spread of trends between individuals and communities to inform marketing strategies.

### 3.3 The infrastructure behind big data

Big-data analytics requires not just algorithms and data, but also physical platforms where the data are stored and analyzed. The related security services used for personal data (see Sections 4.1 and 4.2) are also an essential component of the infrastructure. Once available only to large organizations, this class of infrastructure is now available through “the cloud” to small businesses and to individuals. To the extent that the software infrastructure is widely shared, privacy-preserving infrastructure services can also be more readily used.

#### 3.3.1 Data centers

One way to think about big-data platforms is in physical units of “data centers.” In recent years, data centers have become almost standard commodities. A typical data center is a large, warehouse-like building on a concrete slab the size of a few football fields. It is located with good access to cheap electric power and to a fiber-optic, Internet-backbone connection, usually in a rural or isolated area. The typical center consumes 20–40 megawatts of power (the equivalent of a city with 20,000–40,000 residents) and today houses some tens of thousands of servers and hard-disk drives, totaling some tens of petabytes.<sup>96</sup> Worldwide, there are roughly 6000 data centers of this scale, about half in the United States.<sup>97</sup>

Data centers are the physical locus of big data in all its forms. Large data collections are often replicated in multiple data centers to improve both performance and robustness. There is a growing marketplace in selling data-center services.

Specialized software technology allows the data in multiple data centers (and spread across tens of thousands of processors and hard-disk drives) to cooperate in performing the tasks of data analytics, thereby providing both scaling and better performance. For example, MapReduce (originally a proprietary technology of Google, but now a term used generically) is a programming model for parallel operations across a practically unlimited number of processors; Hadoop is a popular open-source programming platform and program library based on the same ideas; NoSQL (the name derived from “*not* Structured Query Language”) is a set of database technologies that relaxes many of the restrictions of traditional, “relational” databases and allows for better scalability across the many processors in one or more data centers. Contemporary research is aimed at the next generation beyond Hadoop. One path is represented by Accumulo, initiated by the National Security Agency and transitioned to the open-source Apache community.<sup>98</sup> Another is the Berkeley Data Analytics Stack, an open-source platform that outperforms Hadoop by a factor of 100 for memory-intensive data analytics and is being used by such companies as Foursquare, Conviva, Klout, Quantifind, Yahoo, and Amazon Web Services.<sup>99</sup> Sometimes termed “NoHadoop” (to parallel the movement from SQL to NoSQL), technologies that fit this trend include Google’s Dremel, MPI (typically used in supercomputing), Pregel (for graphs), and Cloudscale (for real-time analytics).

<sup>96</sup> A petabyte is  $10^{15}$  bytes. One petabyte could store the individual genomes of the entire U.S. population. The human brain has been estimated to have a capacity of 2.5 petabytes.

<sup>97</sup> McLellan, Charles, “The 21<sup>st</sup> Century Data Center: An Overview,” *ZDNet*, April 2, 2013. <http://www.zdnet.com/the-21st-century-data-center-an-overview-7000012996/>

<sup>98</sup> See: <http://accumulo.apache.org/>

<sup>99</sup> See: <https://amplab.cs.berkeley.edu/software/>

### 3.3.2 The cloud

The “cloud” is not just the world inventory of data centers (although much of the public may think of it as such). Rather, one way of understanding the cloud is as a set of platforms and services *made possible* by the physical commoditization of data centers. When one says that data are “in the cloud,” one refers not just to the physical hard-disk drives that exist (somewhere!) with the data, but also to the complex infrastructure of application programs, middleware, networking protocols, and (not least) business models that allow that data to be ingested, accessed, and utilized, all with costs that are competitively allocated. The commercial entities that, in aggregate, provision the cloud exist in an ecosystem that has many hierarchical levels and many different coexisting models of value added. There may be several handoffs of responsibility between the end user and the physical data center.

Today’s cloud providers offer some security benefits (and through that, privacy benefits) as compared to yesterday’s conventional corporate data centers or small-business computers.<sup>100</sup> These services may include better physical protection and monitoring, as well as centralized support staffing, training, and oversight. Cloud services also pose new challenges for security, a subject of current research. Both benefits and risks come from the centralization of resources: More data are held by a given entity (albeit distributed across multiple servers or sites), and a cloud provider can perform better than separately held data centers by applying high standards to recruiting and managing people and systems.

Usage of the cloud and individual interactions with it (whether witting or not) are expected to increase dramatically in coming years. The rise of both mobile apps,<sup>101</sup> reinforcing the use of cell phones and tablets as platforms, and broadly distributed sensors is associated with the growing use of cloud systems for storing, processing, and otherwise acting on information contributed by dispersed devices. Although progress in the mobile environment improves the usability of mobile cloud applications, it may be detrimental to privacy to the extent that it more effectively hides information exchange from the user. As more core mobile functionality is transitioned to the cloud, larger amounts of information will be exchanged, and users may be surprised by the nature of the information that no longer remains localized to their cell phone. For example, cloud-based screen rendering (or “virtualized screens”) for cell phones would mean that the images shown on a cell-phone screen will actually be calculated on the cloud and transmitted to the mobile device. This means all the images on the screen of the mobile device can be accessed and manipulated from the cloud.

Cloud architectures are also being used increasingly to support big-data analytics, both by large enterprises (e.g., Google, Amazon, eBay) and by small entities or individuals who make ad hoc or routine use of public cloud platforms (e.g., Amazon Web Services, Google Cloud Platform, Microsoft Azure) in lieu of acquiring their own infrastructure. Social-media services such as Facebook and Twitter are deployed and analyzed by their providers using cloud systems. These uses represent a kind of democratization of analytics, with the potential to facilitate new businesses and more. Prospects for the future include exploration of options for federating or

<sup>100</sup> Cloud Security Alliance, “Big Data Working Group: Comment on Big Data and the Future of Privacy,” March 2014. [https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Comment\\_on\\_Big\\_Data\\_Future\\_of\\_Privacy.pdf](https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Comment_on_Big_Data_Future_of_Privacy.pdf)

<sup>101</sup> Qi, H. and A. Gani, “Research on mobile cloud computing: Review, trend and perspectives,” *Digital Information and Communication Technology and its Applications (DICTAP)*, 2012 Second International Conference on, 2012.



interconnecting cloud applications and for reducing some of the heterogeneity in application-programming interfaces for cloud applications.<sup>102</sup>

---

<sup>102</sup> Jeffery, K. et al., "A vision for better cloud applications," *Proceedings of the 2013 International Workshop on Multi-Cloud Applications and Federated Clouds*, Prague, Czech Republic, MODAClouds, ACM Digital Library, April 22-23, 2013.



## 4. Technologies and Strategies for Privacy Protection

Data come into existence, are collected, and are possibly processed immediately (including adding “metadata”), possibly communicated, possibly stored (locally, remotely, or both), possibly copied, possibly analyzed, possibly communicated to users, possibly archived, possibly discarded. Technology at any of these stages can affect privacy positively or negatively.

This chapter focuses on the positive and assesses some of the key technologies that can be used in service of the protection of privacy. It seeks to clarify the important distinctions between privacy and (cyber-)security, as well as the vital, but yet limited, role that encryption technology can play. Some older techniques, such as anonymization, while valuable in the past, are seen as having only limited future potential. Newer technologies, some entering the marketplace and some requiring further research, are summarized.

### 4.1 The relationship between cybersecurity and privacy

Cybersecurity is a discipline, or set of technologies, that seeks to enforce policies relating to several different aspects of computer use and electronic communication.<sup>103</sup> A typical list of such aspects would be

- identity and authentication: Are you who you say you are?
- authorization: What are you allowed to do?
- availability: Can attackers interfere with authorized functions?
- confidentiality: Can data or communications be (passively) copied by someone not authorized to do so?
- integrity: Can data or communications be (actively) changed or manipulated by someone not authorized?
- non-repudiation, auditability: Can actions (payments may provide the best example) later be shown to have occurred?

Good cybersecurity enforces policies that are precise and unambiguous. Indeed, such clarity of policy, expressible in mathematical terms, is a necessary prerequisite for the Holy Grail of cybersecurity, “provably secure” systems. At present, provable security exists only in very limited domains, for example, for certain functions on some kinds of computer chips. It is a goal of cybersecurity research to extend the scope of provably secure systems to larger and larger domains. Meanwhile, practical cybersecurity draws on the emerging principles of such research, but it is guided even more by practical lessons learned from known failures of cybersecurity. The realistic goal is that the practice of cybersecurity should be continuously improving so as to be, in most places and at most of the time, ahead of the evolving threat.

Poor cybersecurity is clearly a threat to privacy. Privacy can be breached by failure to enforce confidentiality of data, by failure of identity and authentication processes, or by more complex scenarios such as those compromising availability.

<sup>103</sup> PCAST has addressed issues in cybersecurity, both in reviewing the NITRD programs and directly in a 2013 report, *Immediate Opportunities for Strengthening the Nation’s Cybersecurity*.

[http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast\\_cybersecurity\\_nov-2013.pdf](http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf)

Security and privacy share a focus on malice. The security of data can be compromised by inadvertence or accident, but it can also be compromised because some party acted knowingly to achieve the compromise – in the language of security, committed an attack. Substituting the words “breach” or “invasion” for “compromise” or “attack,” the same concepts apply to privacy.

Even if there were perfect cybersecurity, however, privacy would remain at risk. Violations of privacy are possible even when there is no failure in computer security. If an authorized individual chooses to misuse (e.g., disclose) data, what is violated is privacy policy, not security policy. Or, as we have discussed (see Section 3.1.1), privacy may be violated by the fusion of data – even if performed by authorized individuals on secure computer systems.<sup>104</sup>

Privacy is different from security in other respects. For one thing, it is harder to codify privacy policies precisely. Arguably this is because the presuppositions and preferences of human beings have greater diversity than the useful scope of assertions about computer security. Indeed, how to codify human privacy preferences is an important, nascent area of research.<sup>105</sup>

When people provide assurance (at some level) that a computer system is secure, they are saying something about applications that are not yet invented: They are asserting that technological design features already in the machine today will prevent such application programs from violating pertinent security policies in that machine, even tomorrow.<sup>106</sup> Assurances about privacy are much more precarious. Since not-yet-invented applications will have access to not-yet-imagined new sources of data, as well as to not-yet-discovered powerful algorithms, it much harder to provide, today, technological safeguards against a new route to violation of privacy tomorrow. Security deals with tomorrow’s threats against today’s platforms. That is hard enough. But privacy deals with tomorrow’s threats against *tomorrow’s* platforms, since those “platforms” comprise not just hardware and software, but also new kinds of data and new algorithms.

Computer scientists often work from the basis of a formal policy for security, just as engineers aim to describe something explicitly so that they can design specific ways to deal with it by purely technical means. As more computer scientists begin to think about privacy, there is increasing attention to formal articulation of privacy policy.<sup>107</sup> To caricature, you have to know what you are doing to know whether what you are doing is doing the right thing.<sup>108</sup> Research addressing the challenges of aligning regulations and policies with software

<sup>104</sup> There are also choices in the design and implementation of security mechanisms that affect privacy. In particular, authentication or the attempt to demonstrate identity at some level can be done with varying degrees of disclosure. See, for example: Computer Science and Telecommunications Board, *Who Goes There: Authentication Through the Lens of Privacy*, National Academies Press, 2003.

<sup>105</sup> Such research can inform efforts to automate the checking of compliance with policies and/or associated auditing.

<sup>106</sup> This future-proofing remains hard to achieve; PCAST’s cybersecurity report advocated approaches that would be more durable than the kinds of check-lists that are easily rendered obsolete. See:

[http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast\\_cybersecurity\\_nov-2013.pdf](http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf)

<sup>107</sup> See, for example: (1) Breaux, Travis D., and Ashwini Rao, “Formal Analysis of Privacy Requirements Specifications for Multi-Tier Applications,” 21<sup>st</sup> IEEE Requirements Engineering Conference (RE 2013), Rio de Janeiro, Brazil, July 2013. [http://www.cs.cmu.edu/~agrao/paper/Analysis\\_of\\_Privacy\\_Requirements\\_Facebook\\_Google\\_Zynga.pdf](http://www.cs.cmu.edu/~agrao/paper/Analysis_of_Privacy_Requirements_Facebook_Google_Zynga.pdf) (2) Feigenbaum, Joan, et al., “Towards a Formal Model of Accountability,” *New Security Paradigms Workshop 2011*, Marin County, CA, September 12-15, 2011. <http://www.nspw.org/papers/2011/nspw2011-feigenbaum.pdf>

<sup>108</sup> Landwehr, Carl, “Engineered Controls for Dealing with Big Data,” Chapter 10, in Lane, Julia, et al., *Privacy, Big Data, and the Public Good*, Cambridge University Press, 2014.

specifications includes formal languages to express policies and system requirements; tools to reason about conflicts, inconsistencies, and ambiguities within and among policies and software specifications; methods to enable requirements engineers, business analysts, and software developers to analyze and refine policy into measurable system specifications that can be monitored over time; formalizing and enforcing privacy through auditing and accountability systems; privacy compliance in big-data systems; and formalizing and enforcing purpose restrictions.

## 4.2 Cryptography and encryption

Cryptography comprises a set of algorithms and system-design principles, some well-developed and others nascent, for protecting data. Cryptography is a field of knowledge whose products are encryption technology. With well-defined protocols, encryption technology is an inhibitor to compromising privacy, but it is not a “silver bullet.”<sup>109</sup>

### 4.2.1 Well established encryption technology

Using cryptography, readable data of any kind, termed plaintext, are transformed into what are, for all intents and purposes, incomprehensible strings of provably random bits, so-called cryptotext. Cryptotext requires no security protection of any kind. It can be stored in the cloud or sent anywhere that is convenient. It can be sent promiscuously to both the NSA and Russian FSB. If they have only cryptotext – and if it was properly generated in a precise mathematical sense – it is useless to them. They can neither read the data nor compute with it. What is needed to decrypt, to turn cryptotext back into the original plaintext, is a “key,” which is in practice a string of bits that is supposed to be known to (or computable by) only authorized users. Only with the key can encrypted data be used, i.e., their value read.

In the context of protecting privacy, it is primarily not the cryptography that is of concern.<sup>110</sup> Rather, compromises of data will occur in one of two main ways:

- Data can be stolen, or mistakenly shared, before they have been encrypted or after they have been decrypted. Many attacks on supposedly encrypted data are actually attacks on machines that contain – however briefly – unencrypted plaintext. For example, in Target’s 2013 breach of one hundred million debit card number and personal-identification numbers (PINs), the PINs were present in unencrypted form only ephemerally. They were stolen nonetheless.<sup>111</sup>
- Keys must be authorized, generated, distributed, and used. At every stage of a key’s life, it is potentially open to compromise or misuse that can ultimately compromise the data that the key was intended to protect. No system based on encryption is secure, of course, if persons with access to private keys can be coerced into sharing them.

<sup>109</sup> The use of this term in computing originated with what is now viewed as a classic article: Brooks, Fred P., “No silver bullet – Essence and Accidents of Software Engineering”, *IEEE Computer* 20:4, April 1987, pp. 10-19.

<sup>110</sup> Attacks that compromise the hardware or software that does the encrypting (for example, the promulgation of intentionally weak cryptography standards) can be considered to be a variant of attacks that reveal plaintext.

<sup>111</sup> “Krebs on Security, collected posts on Target data breach,” 2014, <http://krebsonsecurity.com/tag/target-data-breach/>

Until the 1970s, keys were distributed physically, on paper or computer media, protected by registered mail, armed guards, or anything in between. The invention of “public-key cryptography”<sup>112</sup> changed everything. Public-key cryptography, as the name implies, allows individuals to broadcast publicly their personal key. But this public key is only an encryption key, useful for turning plaintext into ciphertext that is meaningless to others. Its corresponding “private key,” used to transform ciphertext to plaintext, is still kept secret by the recipient. Public-key cryptography thus turns the problem of key distribution into a problem of identity determination. Alice’s messages (encrypted data transmissions) to Bob are completely protected by Bob’s public key – but only if Alice is certain that it is really *Bob’s* public key that she is using, and not the public key of someone merely masquerading as Bob.

Luckily, public-key cryptography also provides some techniques for helping to establish identity, namely the electronic “signing” of messages to document their authenticity. Electronic signatures, in turn, enable messages of the form “I, a person of authority known as X, certify that the following is really the public key of subordinate person Y. (Signed) X.” Messages like this are termed certificates. Certificates can be cascaded, with A certifying the identity of B, who certifies C, and so on. Certificates essentially transform the identity problem from one of validating the identity of millions of possible Y’s to validating the identity of much smaller number of top-level certificate authorities (CAs). Yet it is a matter of concern that more than 100 top-level CAs are widely recognized (e.g., accepted by most all web browsers), because there may be several intermediate steps in the hierarchy of certificates from a CA to a user, and at every step a private key must be protected by some signer on some computer. The compromise of this private key potentially compromises the privacy of all users lower down the chain – because forged certificates of identity can now be created. Such exploits have been seen. For example, the 2011 apparent theft of a Dutch CA’s private key compromised the privacy of potentially all government records in the Netherlands.<sup>113,114</sup>

Many major companies have recently introduced or strengthened their use of encryption to transmit data.<sup>115</sup> Some are now using “(perfect) forward secrecy,” a variant of public-key cryptography that ensures that the compromise of an individual’s private key can compromise only messages that he receives subsequently, while the confidentiality of past conversations is maintained, even if their ciphertext was previously recorded by the same eavesdropper now in possession of the purloined private key.<sup>116</sup>

#### 4.2.2 Encryption frontiers

The technologies thus far mentioned enable the protection of data both in storage and in transit, allowing those data to be fully decrypted by users who either (i) have the right key already (as might be the case for persons

<sup>112</sup> Public-key encryption originated through the secret work of British mathematicians at the U.K.’s Government Communications Headquarters (GCHQ), an organization roughly analogous to the NSA, and received broader attention through the independent work by researchers including Whitfield Diffie and Martin Hellman in the United States.

<sup>113</sup> Fisher, Dennis, “Final Report on DigiNotar Hack Shows Total Compromise of CA Servers,” *ThreatPost*, October 31, 2012. <http://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170>.

<sup>114</sup> It is not publicly known whether or not the earlier 2010 compromise of servers belonging to VeriSign, a much larger CA, led to compromises of certificates or signing authorities. Bradley, Tony, “VeriSign Hacked: What We Don’t Know Might Hurt Us,” *PC World*, February 2, 2012.

[http://www.pcworld.com/article/249242/verisign\\_hacked\\_what\\_we\\_dont\\_know\\_might\\_hurt\\_us.html](http://www.pcworld.com/article/249242/verisign_hacked_what_we_dont_know_might_hurt_us.html)

<sup>115</sup> A sample report-card: <https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what#crypto-chart>

<sup>116</sup> Diffie, Whitfield, et al., “Authentication and Authenticated Key Exchanges” *Designs, Codes and Cryptography* 2:2, June 1992, pp.107-125.

storing data for their own later use), or (ii) are authorized by the data owner and have identities certified by a CA that is itself trusted by the data owner. A frontier of cryptography research, with some inventions now starting to make it into practice, is how to create different kinds of keys, ones which give only limited access of various kinds, or which allow messages to be sent to classes of individuals without knowing in advance exactly who they may be.

For example, “identity-based encryption” and “attribute-based encryption” are ways of sending a message, or protecting a file of data, for the exclusive use of “a person named Ramona Q. Doe who was born on May 23, 1980,” or for “anyone with the job title ombudsman, ombudsperson, or consumer advocate.” These techniques require a trusted third party (essentially a certificate authority), but the messages themselves do not need to pass through the hands of that third party. These tools are in early stages of adoption.

“Zero-knowledge” systems allow encrypted data to be queried for certain higher-level abstractions without revealing the low-level data. For example, a website operator could verify that a user is over age 21 without learning the user’s actual birthdate. What is remarkable is that this can be done in a way that proves mathematically that the user is not lying about his age: The operator learns with mathematical certainty that a certificate (signed by some CA of course!) attests to the user’s birthdate, without ever actually seeing that certificate. Zero-knowledge systems are just beginning to be commercialized in simple cases. They are not foreseeably extendable to complex and unstructured situations, such as what might be needed for the research mining of health-record data from non-consenting patients.

In some simpler domains, for example location privacy, practical cryptographic protection is closer to reality. The typical case might be that a group of friends want to know when they are close to one another, but without sharing their actual locations with any third party. Applications like this are, of course, much simpler if there is a trusted third party, as is *de facto* the case for most such commercial applications today.

Homomorphic encryption is a research area that goes beyond the mere querying of encrypted databases to actual computations (e.g., the collection of statistics) using encrypted data without ever decrypting it. These techniques are far from being practical, and they are unlikely to provide policy options on the timescale relevant to this report.

In secure multi-party computation, which is related to homomorphic encryption and is of particular interest in the financial sector, computation may be done on distributed data stores that are encrypted. Although individual data are kept private using “collusion-robust” encryption algorithms, data can be used to calculate general statistics. Parties that each know some private data use a protocol that generates useful results based on both information they know and information they do not know, without revealing to them data they do not already know.

Differential privacy, a comparatively new development related to but different from encryption, aims to maximize the accuracy of database queries or computations while minimizing the identifiability of individuals with records in the database, typically via obfuscation of query results (for example, by the addition of spurious information or “noise”).<sup>117</sup> As with other obfuscation approaches, there is a tradeoff between data anonymity

<sup>117</sup> (1) Dwork, Cynthia, “Differential Privacy,” 33rd International Colloquium on Automata, Languages and Programming, 2006. (2) Dwork, Cynthia, “A Firm Foundation for Private Data Analysis,” *Communications of the ACM*, 54.1, 2011.

and the accuracy and utility of the query outputs. These ideas are far from practical application, except insofar as they may enable the risks of allowing any queries at all to be better assessed.

### 4.3 Notice and consent

Notice and consent is, today, the most widely used strategy for protecting consumer privacy. When the user downloads a new app to his or her mobile device, or when he or she creates an account for a web service, a notice is displayed, to which the user must positively indicate consent before using the app or service. In some fantasy world, users actually read these notices, understand their legal implications (consulting their attorneys if necessary), negotiate with other providers of similar services to get better privacy treatment, and only then click to indicate their consent. Reality is different.<sup>118</sup>

Notice and consent fundamentally places the burden of privacy protection on the individual – exactly the opposite of what is usually meant by a “right.” Worse yet, if it is hidden in such a notice that the provider has the right to share personal data, the user normally does not get any notice from the next company, much less the opportunity to consent, even though use of the data may be different. Furthermore, if the provider changes its privacy notice for the worse, the user is typically not notified in a useful way.

As a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data. It is simply too complicated for the individual to make fine-grained choices for every new situation or app. Nevertheless, since notice and consent is so deeply rooted in current practice, some exploration of how its usefulness might be extended seems warranted.

One way to view the problem with notice and consent is that it creates a non-level playing field in the implicit privacy negotiation between provider and user. The provider offers a complex take-it-or-leave-it set of terms, backed by a lot of legal firepower, while the user, in practice, allocates only a few seconds of mental effort to evaluating the offer, since acceptance is needed to complete the transaction that was the user’s purpose, and since the terms are typically difficult to comprehend quickly. This is a kind of market failure. In other contexts, market failures like this can be mitigated by the intervention of third parties who are able to represent significant numbers of users and negotiate on their behalf. Section 4.5.1 below suggests how such intervention might be accomplished.

### 4.4 Other strategies and techniques

#### 4.4.1 Anonymization or de-identification

Long used in health-care research and other research areas involving human subjects, anonymization (also termed de-identification) applies when the data, standing alone and without an association to a specific person, do not violate privacy norms. For example, you may not mind if your medical record is used in research as long as you are identified only as Patient X and your actual name and patient identifier are stripped from that record.

Anonymization of a data record might seem easy to implement. Unfortunately, it is increasingly easy to defeat anonymization by the very techniques that are being developed for many legitimate applications of big data. In

<sup>118</sup> Gindin, Susan E., “Nobody Reads Your Privacy Policy or Online Contract: Lessons Learned and Questions Raised by the FTC’s Action against Sears,” *Northwestern Journal of Technology and Intellectual Property* 1:8, 2009-2010.

general, as the size and diversity of available data grows, the likelihood of being able to re-identify individuals (that is, re-associate their records with their names) grows substantially.<sup>119</sup>

One compelling example comes from Sweeney, Abu, and Winn.<sup>120</sup> They showed in a recent paper that, by fusing public, Personal Genome Project profiles containing zip code, birthdate, and gender with public voter rolls, and mining for names hidden in attached documents, 84-97 percent of the profiles for which names were provided were correctly identified.

Anonymization remains somewhat useful as an added safeguard, but it is not robust against near-term future re-identification methods. PCAST does not see it as being a useful basis for policy. Unfortunately, anonymization is already rooted in the law, sometimes giving a false expectation of privacy where data lacking certain identifiers are deemed not to be personally identifiable information and therefore not covered by such laws as the Family Educational Rights and Privacy Act (FERPA).

#### 4.4.2 Deletion and non-retention

It is an evident good business practice that data of all kinds should be deleted when they are no longer of value. Indeed, well-run companies often mandate the destruction of some kinds of records (both paper and electronic) after specified periods of time, often because they see little benefit in keeping the records as well as potential cost in producing them. For example, employee emails, which may be subject to legal process by (e.g.) divorce lawyers, are often seen as having negative retention value.

Counter to this practice is the new observation that big data is frequently able to find economic or social value in masses of data that were otherwise considered to be worthless. As the physical cost of retention continues to decrease exponentially with time (especially in the cloud), there will be a tendency in both government and the private sector to hold more data for longer – with obvious privacy implications. Archival data may also be important to future historians, or for later longitudinal analysis by academic researchers.

Only policy interventions will counter this trend. Government can mandate retention policies for itself. To affect the private sector, government may mandate policies where it has regulatory authorities (as for consumer protection, for example). But it can also encourage the development of stricter liability standards for companies whose data, including archived data, cause harm to individuals. A rational response by the private sector would then be to hold fewer data or to protect their use.

The above holds true for privacy-sensitive data about individuals that are held overtly – that is, the holder knows that he has the data and to whom they relate. As was discussed in Section 3.1.2, however, sources of data increasingly contain latent information about individuals, information that becomes known only if the holder expends analytic resources (beyond what may be economically feasible), or that may become knowable only in the future with the development of new data-mining algorithms. In such cases it is practically impossible for the data holder even to surface “all the data about an individual,” much less delete those data on any specified schedule.

<sup>119</sup> De-identification can also be seen as a spectrum, rather than a single approach. See: “Response to Request for Information Filed by U.S. Public Policy Council of the Association for Computing Machinery,” March 2014.

<sup>120</sup> Sweeney, et al., “Identifying Participants in the Personal Genome Project by Name,” *Harvard University Data Privacy Lab*. White Paper 1021-1, April 24, 2013. <http://dataprivacylab.org/projects/pgp/>



The concepts of ephemerality (keeping data only on-the-fly or for a brief period), and transparency (enabling the individual to know what data about him or her are held) are closely related, and with the same practical limitations. While data that are only streamed, and not archived, may have lower risk of future use, there is no guarantee that a violator will play by the supposed rules, as in Target's loss of 100 million debit card PINs, each present only ephemerally (see Section 4.2.1).

Today, given the distributed and redundant nature of data storage, it is not even clear that data *can* be destroyed with any useful degree of assurance. Although research on data destruction is ongoing, it is a fundamental fact that at the moment that data are displayed (in "analog") to a user's eyeballs or ears, they can also be copied ("re-digitized") without any technical protections. The same holds if data are ever made available in unencrypted form to a rogue computer program, one designed to circumvent technical safeguards. Some misinformed public discussion notwithstanding, there is no such thing as automatically self-deleting data, other than in a fully controlled and rule-abiding environment.

As a current example, SnapChat provides the service of delivering ephemeral snapshots (images), visible for only a few seconds, to a designated recipient's mobile device. SnapChat promises to delete past-date snaps from their servers, but it is only a promise. And, they are careful *not* to promise that the intended recipient may not contrive to make an uncontrolled and non-expiring copy. Indeed, the success of SnapChat incentivizes the development of just such copying applications.<sup>121</sup>

From a policymaking perspective, the only viable assumption today, and for the foreseeable future, is that data, once created, are permanent. While their *use* may be regulated, their continued *existence* is best considered conservatively as unalterable fact.

## 4.5 Robust technologies going forward

### 4.5.1 A Successor to Notice and Consent

The purpose of notice and consent is that the user assents to the collection and use of personal data for a stated purpose that is acceptable to that individual. Given the large number of programs and Internet-available devices, both visible and not, that collect and use personal data, this framework is increasingly unworkable and ineffective. PCAST believes that the responsibility for using personal data in accordance with the user's preferences should rest with the provider, possibly assisted by a mutually accepted intermediary, rather than with the user.

How might that be accomplished? Individuals might be encouraged to associate themselves with one of a standard set of privacy preference profiles (that is, settings or choices) voluntarily offered by third parties. For example, Jane might choose to associate with a profile offered by the American Civil Liberties Union that gives particular weight to individual rights, while John might associate with one offered by *Consumer Reports* that gives weight to economic value for the consumer. Large app stores (such as Apple App Store, Google Play, Microsoft Store) for whom reputational value is important, or large commercial sectors such as finance, might choose to offer competing privacy-preference profiles.

<sup>121</sup> See, for example: Ryan Whitwam, "Snap Save for iPhone Defeats the Purpose of Snapchat, Saves Everything Forever," *PC Magazine*, August 12, 2013. <http://apopsout.pcmag.com/apple-ios-iphone-ipad-ipod/314653-snap-save-for-iphone-defeats-the-purpose-of-snapchat-saves-everything-forever>

In the first instance, an organization offering profiles would vet new apps as acceptable or not acceptable within each of their profiles. Basically, they would do the close reading of the provider's notice that the user should, but does not, do. This is not as onerous as it may sound: While there are millions of apps, the most popular downloads are relatively few and are concentrated in a relatively small number of portals. The "long tail" of apps with few customers each might initially be left as "unrated."

Simply by vetting apps, the third-party organizations would automatically create a marketplace for the negotiation of community standards for privacy. To attract market share, providers (especially smaller ones) could seek to qualify their offerings in as many privacy-preference profiles, offered by as many different third parties, as they deem feasible. The Federal government (e.g., through the National Institute of Standards and Technology) could encourage the development of standard, machine-readable interfaces for the communication of privacy implications and settings between providers and assessors.

Although human professionals could do the vetting today using policies expressed in natural language, it would be desirable in the future to automate that process. To do that, it would be necessary to have formalisms to specify privacy policies and tools to analyze software to determine conformance to those policies. But that is only part of the challenge. A greater challenge is to make sure the policy language is sufficiently expressive, the policies are sufficiently rich, and conformance tests are sufficiently powerful. Those requirements lead to a consideration of context and use.

#### 4.5.2 Context and Use

The previous discussion, particularly that of Sections 3.1 and 3.2, illustrates PCAST's belief that a focus on the collection, storage, and retention of electronic personal data will not provide a technologically robust foundation on which to base future policy. Among the many authors that have touched on these issues, Kagan and Abelson explain why access control does not suffice to protect privacy.<sup>122</sup> Mundie gives a cogent and more complete explanation of this issue and advocates that privacy protection is better served by controlling the use of personal data, broadly construed, including metadata and data derived from analytics than by controlling collection.<sup>123</sup> In a complementary vein, Nissenbaum explains that both the context of usage and the prevailing social norms contribute to acceptable use.<sup>124</sup>

To implement in a meaningful way the application of privacy policies to the use of personal data for a particular purpose (i.e., in context), those policies need to be associated both with data and with the code that operates on the data. For example, it must be possible to ensure that only apps with particular properties can be applied to certain data. The policies might be expressed in what computer scientists call natural language (plain English or the equivalent) and the association done by the user, or the policies might be stated formally and their association and enforcement done automatically. In either case, there must also be policies associated with the outputs of the computation, since they are data as well. The privacy policies of the output data must be computed from the policies associated with the inputs, the policies associated with the code, and the intended use of the outputs (i.e., the context). These privacy properties are a kind of metadata. To achieve a reasonable level of reliability, their implementation must be tamper-proof and "sticky" when data are copied.

<sup>122</sup> Abelson, Hal and Lalana Kagal, "Access Control is an Inadequate Framework for Privacy Protection," *W3C Workshop on Privacy for Advanced Web APIs 12/13*, July 2010, London. <http://www.w3.org/2010/api-privacy-ws/papers.html>

<sup>123</sup> Mundie, Craig, "Privacy Pragmatism: Focus on Data Use, Not Data Collection," *Foreign Affairs*, March/April, 2014.

<sup>124</sup> Nissenbaum, H., "Privacy in Context: Technology, Policy, and the Integrity of Social Life," *Stanford Law Books*, 2009.

There has been considerable research in areas that would contribute to such a capability, some of which is beginning to be commercialized. There is a history of using metadata (“tags” or “attributes”) in database systems to control use. While the formalization of privacy policies and their synthesis is a research topic,<sup>125</sup> manual interpretation of such policies and the human determination of usage tags can be found in recent products. Identity management systems (to authenticate users and their roles, i.e., their context) are also evident both in research<sup>126</sup> and in practice.<sup>127</sup>

Commercial privacy systems for implementing use control exist today under the name of Trusted Data Format (TDF) implementations, developed principally for the United States intelligence community.<sup>128</sup> TDF operates at the file level. The systems are primarily being implemented on a custom basis by large consulting firms, often assembled from open-source software components. Customers today are primarily government agencies, such as Federal intelligence agencies or local-government criminal intelligence units, or large commercial companies in vertically integrated industries like financial services and pharmaceutical companies looking to improve their accountability and auditing capabilities. Consulting services that have expertise in building such systems include, for example, Booz Allen, Ernst & Young, IBM, Northrop Grumman, and Lockheed; product-based companies like Palantir and new startups pioneering internal usage auditing, policy analytics, and policy reasoning engines have such expertise, as well. With sufficient market demand, more widespread market penetration could happen in the next five years. Market penetration would be further accelerated if the leading cloud-platform providers like Amazon, Google, and Microsoft implemented usage-controlled system technologies in their offerings. Wider-scale use through the government would help motivate the creation of off-the-shelf standard software.

#### 4.5.3 Enforcement and deterrence

Privacy policies and the control of use in context are only effective to the extent that they are realized and enforced. Technical measures that increase the probability that a violator is caught can be effective only when there are regulations and laws with civil or criminal penalties to deter the violators. Then there is both deterrence of harmful actions and incentive to deploy privacy-protecting technologies.

It is today straightforward technically to associate metadata with data, with varying degrees of granularity ranging from an individual datum, to a record, to an entire collection. These metadata can record a wealth of auditable information, for example, provenance, detailed access and use policies, authorizations, logs of actual access and use, and destruction dates. Extending such metadata to derived or shared data (secondary use) together with privacy-aware logging can facilitate auditing. Although the state of the art is still somewhat ad hoc, and auditing is often not automated, so-called accountable systems are beginning to be deployed (Section

<sup>125</sup> See references at footnote 107 and also: (1) Weitzner, D.J., et al., “Information Accountability,” *Communications of the ACM*, June 2008, pp. 82-87. (2) Tschantz, Michael Carl, Anupam Datta, and Jeannette M. Wing, “Formalizing and Enforcing Purpose Restrictions in Privacy Policies,” <http://www.andrew.cmu.edu/user/danupam/TschantzDattaWing12.pdf>

<sup>126</sup> For example, at Carnegie Mellon University, Lorrie Cranor directs the CyLab Usable Privacy and Security Laboratory (<http://cups.cs.cmu.edu/>). Also, see *2nd International Workshop on Accountability: Science, Technology and Policy*, MIT Computer Science and Artificial Intelligence Laboratory, January 29-30, 2014. <http://dig.csail.mit.edu/2014/AccountableSystems2014/>

<sup>127</sup> Oracle’s eXtensible Access Control Markup Language (XACML) has been used to implement attribute-based access controls for identity management systems. (Personal communication, Mark Gorenberg and Peter Guerra of Booz Allen)

<sup>128</sup> Office of the Director of National Intelligence, “IC CIO Enterprise Integration & Architecture: Trusted Data Format.” <http://www.dni.gov/index.php/about/organization/chief-information-officer/trusted-data-format>

4.5.2). The ability to detect violations of privacy policies, particularly if the auditing is automated and continuous, can be used both to deter privacy violations and to ensure that violators are punished.

In the next five years, with regulation or market-driven encouragement, the large cloud-based infrastructure systems (e.g., Google, Amazon, Microsoft, Rackspace) could, as one example, incorporate the data-provenance and usage-compliance aspects of accountable systems into their cloud application-programming interfaces (APIs) and additionally provide APIs for policy awareness. These capabilities could then readily be included in open-source-based systems like Open Stack (associated with Rackspace)<sup>129</sup> and other provider platforms. Applications intended to run on such cloud-based systems could be built with privacy concepts “baked into them,” even when they are developed by small enterprises or individual developers.

#### 4.5.4 Operationalizing the Consumer Privacy Bill of Rights

In February 2012, the Administration issued a report setting forth a Consumer Privacy Bill of Rights (CPBR). The CPBR addresses commercial (not public sector) uses of personal data and is a strong statement of American privacy values.

For purposes of this discussion, the principles embodied in CPBR can be divided into two categories. First, there are obligations for data holders, analyzers, or commercial users. These are passive from the consumer’s standpoint – the obligations should be met whether or not the consumer knows, cares, or acts. Second, and different, there are consumer empowerments, things that the consumer should be empowered to initiate actively. It is useful here to rearrange the CPBR’s principles by category.

In the category of obligations are these elements:

- Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- Security: Consumers have a right to secure and responsible handling of personal data.
- Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

In the category of consumer empowerments are these elements:

- Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.

PCAST endorses as sound the principles underlying CPBR. Because of the rapidly changing technologies associated with big data, however, effective operationalization of CPBR is at risk. Up to now, debate over how to operationalize CPBR has focused on the collection, storage, and retention of data, with an emphasis on the

<sup>129</sup> See: <http://www.openstack.org/>

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

“small-data” contexts that motivated CPBR development. But, as discussed at multiple places in this report (e.g., Sections 3.1.2, 4.4 and 4.5.2), PCAST believes that such a focus will not provide a technologically robust foundation on which to base future policy that also applies to big data. Further, the increasing complexity of applications and uses of data undermines even a simple concept like “notice and consent.”

PCAST believes that the principles of CPBR can readily be adapted to a more robust regime based on recognizing and controlling harmful uses of the data. Some specific suggestions follow.

Turn first to the rights classified above as obligations on the data holder.

The principle of Respect for Context needs augmentation. As this report has repeatedly discussed, there are instances in which personal data are not provided by the customer. Such data may emerge as a product of analysis well after the data were collected and after they may have passed through several hands. While the intent of the right is appropriate, namely that data be used for legitimate purposes that do not produce certain adverse consequences or harms to individuals, the CPBR’s articulation in which “consumers provide the data” is too limited. This right needs to state in some way that data about an individual – however acquired – not be used so as to cause certain adverse consequences or harms to that individual. (See Section 1.4 for a possible list of adverse consequences and harms that might be subject to some regulation.)

As initially conceived, the right to Focused Collection was to be achieved by techniques like de-identification and data deletion. As discussed in Section 4.4.1, however, de-identification (anonymization) is not a robust technology for big data in the face of data fusion; in some instances, there may be compelling reasons to retain data for beneficial purposes. This right should be about use rather than collection. It should emphasize utilizing best practices to prevent inappropriate use of data during the data’s whole life cycle, rather than depending on de-identification. It should not depend on a company’s being able itself to recognize “all” the data about a consumer that it holds, which is increasingly technically infeasible.

The principles underlying CPBR’s Security and Accountability remain valid in a use-based regime. They need to be applied throughout the value chain that includes data collection, analysis, and use.

Turn next to the rights here classified as consumer empowerments.

Where consumer empowerments have become practically impossible for the consumer to exercise meaningfully, they need to be recast as obligations of the commercial entity that actually uses the data or products of data analysis. This applies to the CPBR’s principles of Individual Control and of Transparency.

Section 4.3 explained how the non-obvious nature of big data’s products of analysis make it all but impossible for an individual to make fine-grained privacy choices for every new situation or app. For the principle of Individual Control to have meaning, PCAST believes that the burden should no longer fall on the consumer to manage privacy for each company with which the consumer interacts by a framework like “notice and consent.” Rather, each company should take responsibility for conforming its uses of personal data to a personal privacy profile designated by the consumer and made available to that company (including from a third party designated by the consumer). Section 4.5.1 proposed a mechanism for this change in responsibility.

Transparency (in the sense of disclosure of privacy practices) suffers from many of the same problems. Today, the consumer receives an unhelpful blizzard of privacy-policy notifications, many of which say, in essence, “we

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

providers can do anything we want.”<sup>130</sup> As with Individual Control, the burden of conforming to a consumer’s stated personal-privacy profile should fall on the company, with notification to the consumers by a company if their profile precludes that company’s accepting their business. Since companies do not like to lose business, a positive market dynamic for competing privacy practices would thus be created.

For the right of Access and Accuracy to be meaningful, personal data must include the fruits of data analytics, not just collection. However, as this report has already explained (Section 4.4.2), it is not always possible for a company to “know what it knows” about a consumer, since that information may be unrecognized in the data; or it may become identifiable only in the future, when data sets are combined using new algorithms. When, however, the personal character of data is apparent to a company by virtue of its use of the data, its obligation to provide means for the correction of errors should be triggered. Consumers should have an expectation that companies will validate and correct data stemming from analysis and, since not all errors will be corrected, will also take steps to minimize the risk of adverse consequences to consumers from the use of inaccurate data. Again, the primary burden must fall on the commercial user of big data and not on the consumer.

---

<sup>130</sup> Lawyers may encourage companies to use over-inclusive language to cover the unpredictable evolution of possibilities described elsewhere in this report, even in the absence of specific plans to use specific capabilities.





## 5. PCAST Perspectives and Conclusions

Breaches of privacy can cause harm to individuals and groups. It is a role of government to prevent such harm where possible, and to facilitate means of redress when the harm occurs. Technical enhancements of privacy can be effective only when accompanied by regulations or laws because, unless some penalties are enforced, there is no end to the escalation of the measures-countermeasures “game” between violators and protectors. Rules and regulations provide both deterrence of harmful actions and incentives to deploy privacy-protecting software technologies.

From everything already said, it should be obvious that new sources of big data are abundant; that they will continue to grow; and that they can bring enormous economic and social benefits. Similarly, and of comparable importance, new algorithms, software, and hardware technologies will continue to increase the power of data analytics in unexpected ways. Given these new capabilities of data aggregation and processing, there is inevitably new potential for both the unintentional leaking of both bulk and fine-grained data about individuals, and for new systematic attacks on privacy by those so minded.

Cameras, sensors, and other observational or mobile technologies raise new privacy concerns. Individuals often do not knowingly consent to providing data. These devices naturally pull in data unrelated to their primary purpose. Their data collection is often invisible. Analysis technology (such as facial, scene, speech, and voice recognition technology) is improving rapidly. Mobile devices provide location information that might not be otherwise volunteered. The combination of data from those sources can yield privacy-threatening information unbeknownst to the affected individuals.

It is also true, however, that privacy-sensitive data cannot always be reliably recognized when they are first collected, because the privacy-sensitive elements may be only latent in the data, made visible only by analytics (including those not yet invented), or by fusion with other data sources (including those not yet known). Suppressing the collection of privacy-sensitive data would thus be increasingly difficult, and it would also be increasingly counterproductive, frustrating the development of big data’s socially important and economic benefits.

Nor would it be desirable to suppress the combining of multiple sources and kinds of data: Much of the power of big data stems from this kind of data fusion. That said, it remains a matter of concern that considerable amounts of personal data may be derived from data fusion. In other words, such data can be obtained or inferred without intentional personal disclosure.

It is an unavoidable fact that particular collections of big data and particular kinds of analysis will often have both beneficial and privacy-inappropriate uses. The appropriate use of both the data and the analyses are highly contextual.

Any specific harm or adverse consequence is the result of data, or their analytical product, passing through the control of three distinguishable classes of actor in the value chain:

First, there are *data collectors*, who control the interfaces to individuals or to the environment. Data collectors may collect data from clearly private realms (e.g., a health questionnaire or wearable sensor), from ambiguous situations (e.g., cell-phone pictures or Google Glass videos taken at a party or cameras and microphones placed



in a classroom for remote broadcast), or – increasing in both quantity and quality – data from the “public square,” where privacy-sensitive data may be latent and initially unrecognizable.

Second, there are *data analyzers*. This is where the “big” in big data becomes important. Analyzers may aggregate data from many sources, and they may share data with other analyzers. Analyzers, as distinct from collectors, create uses (“products of analysis”) by bringing together algorithms and data sets in a large-scale computational environment. Importantly, analyzers are the locus where individuals may be profiled by data fusion or statistical inference.

Third, there are *users of the analyzed data* – business, government, or individual. Users will generally have a commercial relationship with analyzers; they will be purchasers or licensees (etc.) of the analyzer’s products of analysis. It is the user who creates desirable economic and social outcomes. But, it is also the user who is the locus of producing actual adverse consequences or harms, when such occur.

### 5.1 Technical feasibility of policy interventions

Policy, as created by new legislation or within existing regulatory authorities, can, in principle, intervene at various stages in the value chain described above. Not all such interventions are equally feasible from a technical perspective, or equally desirable if the societal and economic benefits of big data are to be realized.

As indicated in Chapter 4, basing policy on the control of collection is unlikely to succeed, except in very limited circumstances where there is an explicitly private context (e.g., measurement or disclosure of health data) and the possibility of *meaningful* explicit or implicit notice and consent (e.g., by privacy preference profiles, see Sections 4.3 and 4.5.1), which does not exist today.

There is little technical likelihood that “a right to forget” or similar limits on retention could be meaningfully defined or enforced (see Section 4.4.2). Increasingly, it will not be technically possible to surface “all” of the data about an individual. Policy based on protection by anonymization is futile, because the feasibility of re-identification increases rapidly with the amount of additional data (see Section 4.4.1). There is little, and decreasing, meaningful distinction between data and metadata. The capabilities of data fusion, data mining, and re-identification render metadata not much less problematic than data (see Section 3.1).

Even if direct controls on collection are in most cases infeasible, however, attention to collection practices may help to reduce risk in some circumstances. Such best practices as tracking provenance, auditing access and use, and continuous monitoring and control (see Sections 4.5.2 and 4.5.3) could be driven by partnerships between government and industry (the carrot) and also by clarifying tort law and defining what might constitute negligence (the stick).

Turn next to data analyzers. On the one hand, it may be difficult to regulate them, because their actions do not directly touch the individual (it is neither collection nor use) and may have no external visibility. Mere inference about an individual, absent its publication or use, may not be a feasible target of regulation. On the other hand, an increasing fraction of privacy issues will surface only with the application of data analytics. Many privacy challenges will arise from the analysis of data collected unintentionally that was not, at the time of collection, targeted at any particular individual or even group of individuals. This is because combining data from many sources will become more and more powerful.

It might be feasible to introduce regulation at the “moment of particularization” of data about an individual, or when this is done for some minimum number of individuals concurrently. To be effective such regulation would

need to be accompanied by requirements for tracking provenance, auditing access and use, and using security measures (e.g., robust encryption infrastructure) at all stages of the evolution of data, and for providing transparency, and/or notification, at the moment of particularization.

Big data's "products of analysis" are created by computer programs that bring together algorithms and data so as to produce something of value. It might be feasible to recognize such programs, or their products, in a legal sense and to regulate their commerce. For example, they might not be allowed to be used in commerce (sold, leased, licensed, and so on) unless they are consistent with individuals' privacy elections or other expressions of community values (see Sections 4.3 and 4.5.1). Requirements might be imposed on conformity to appropriate standards of provenance, auditability, accuracy, and so on, in the data they use and produce; or that they meaningfully identify who (licensor vs. licensee) is responsible for correcting errors and liable for various types of harm or adverse consequence caused by the product.

It is not, however, the mere development of a product of analysis that can cause adverse consequences. Those occur only with its actual use, whether in commerce, by government, by the press, or by individuals. This seems the most technically feasible place to apply regulation going forward, focusing at the locus where harm can be produced, not far upstream from where it may barely (if at all) be identifiable.

When products of analysis produce imperfect information that may misclassify individuals in ways that produce adverse consequences, one might require that they meet standards for data accuracy and integrity; that there are useable interfaces that allow an individual to correct the record with voluntary additional information; and that there exist streamlined options for redress, including financial redress, when adverse consequences reach a certain level.

Some harms may affect groups (e.g., the poor or minorities) rather than identifiable individuals. Mechanisms for redress in such cases need to be developed.

There is a need to clarify standards for liability in case of adverse consequences from privacy violations. Currently there is a patchwork of out-of-date state laws and legal precedents. One could encourage the drafting of technologically savvy model legislation on cyber-torts for consideration by the states.

Finally, government may be forbidden from certain classes of uses, despite their being available in the private sector.

## 5.2 Recommendations

PCAST's charge for this study does not ask it to make recommendations on privacy policies, but rather to make a relative assessment of the technical feasibility of different broad policy approaches. PCAST's overall conclusions about that question are embodied in the first two of our recommendations:

### **Recommendation 1. Policy attention should focus more on the actual uses of big data and less on its collection and analysis.**

By actual uses, we mean the specific events where something happens that can cause an adverse consequence or harm to an individual or class of individuals. In the context of big data, these events ("uses") are almost always actions of a computer program or app interacting either with the raw data or with the fruits of analysis of those data. In this formulation, it is not the data themselves that cause the harm, nor the program itself (absent any data), but the confluence of the two. These "use events" (in commerce, by government, or by individuals)

## BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

embody the necessary specificity to be the subject of regulation. Since the purpose of bringing program and data together is to accomplish some identifiable desired task, use events also capture some notion of intent, in a way that data collection by itself or program development by itself may not. The policy question of what kinds of adverse consequences or harms rise to the level of needing regulation is outside of PCAST's charge, but an illustrative set that seem grounded in common American values was provided in Section 1.4.

PCAST judges that alternative big-data policies that focus on the regulation of data collection, storage, retention, a priori limitations on applications, and analysis (absent identifiable actual uses of big data or its products of analysis) are unlikely to yield effective strategies for improving privacy. Such policies are unlikely to be scalable over time as it becomes increasingly difficult to ascertain, about any particular data set, what personal information may be latent in it – or in its possible fusion with every other possible data set, present or future. The related issue is that policies limiting collection and retention are increasingly unlikely to be enforceable by other than severe and economically damaging measures. While there are certain definable classes of data so repugnant to society that their mere possession is criminalized,<sup>131</sup> the information in big data that may raise privacy concerns is increasingly inseparable from a vast volume of the data of ordinary commerce, or government function, or collection in the public square. This dual-use character of information, too, argues for the regulation of use rather than collection.

**Recommendation 2. Policies and regulation, at all levels of government, should not embed particular technological solutions, but rather should be stated in terms of intended outcomes.**

To avoid falling behind the technology, it is essential that policy concerning privacy protection should address the purpose (the “what”) rather than the mechanism (the “how”). For example, regulating disclosure of health information by regulating the use of anonymization fails to capture the power of data fusion; regulating the protection of information about minors by controlling inspection of student records held by schools fails to anticipate the student information capturing by online learning technologies. Regulating control of the inappropriate disclosure of health information or student performance, no matter how the data are acquired is more robust.

PCAST further responds to its charge with the following recommendations, intended to advance the agenda of strong privacy values and the technological tools needed to support them:

**Recommendation 3. With coordination and encouragement from OSTP, the NITRD agencies<sup>132</sup> should strengthen U.S. research in privacy-related technologies and in the relevant areas of social science that inform the successful application of those technologies.**

Some of the technology for protecting uses already exists. Research (and funding for it) is needed, however, in the technologies that help to protect privacy, in the social mechanisms that influence privacy-preserving

---

<sup>131</sup> Child pornography is the most universally recognized example.

<sup>132</sup> NITRD refers to the Networking and Information Technology Research and Development program, whose participating Federal agencies support unclassified research in in advanced information technologies such as computing, networking, and software and include both research- and mission-focused agencies such as NSF, NIH, NIST, DARPA, NOAA, DOE's Office of Science, and the DOD military service laboratories (see [http://www.nitrd.gov/SUBCOMMITTEE/nitrd\\_agencies/index.aspx](http://www.nitrd.gov/SUBCOMMITTEE/nitrd_agencies/index.aspx)). There is research coordination between NITRD and Federal agencies conducting or supporting corresponding classified research.

behavior, and in the legal options that are robust to changes in technology and create appropriate balance among economic opportunity, other national priorities, and privacy protection.

Following up on recommendations from PCAST for increased privacy-related research,<sup>133</sup> a 2013-2014 internal government review of privacy-focused research across Federal agencies supporting research on information technologies suggests that about \$80 million supports either research with an explicit focus on enhancing privacy or research that addresses privacy protection ancillary to some other goal (typically cybersecurity).<sup>134</sup> The funded research addresses such topics as an individual's control over his or her information, transparency, access and accuracy, and accountability. It is typically of a general nature, except for research focusing on the health domain or (relatively new) consumer energy usage. The broadest and most varied support for privacy research, in the form of grants to individuals and centers, comes from the National Science Foundation (NSF), engaging social science as well as computer science and engineering.<sup>135,136</sup>

Research into privacy as an extension or complement to security is supported by a variety of Department of Defense agencies (Air Force Research Laboratory, the Army's Telemedicine and Advanced Technology Research Center, Defense Advanced Research Projects Agency, National Security Agency, and Office of Naval Research) and the Intelligence Advanced Research Projects Activity (IARPA) within the Intelligence Community. IARPA, for example, has hosted the Security and Privacy Assurance Research<sup>137</sup> program, which has explored a variety of encryption techniques. Research at the National Institute for Standards and Technology (NIST) focuses on the development of cryptography and biometric technology to enhance privacy as well as support for federal standards and programs for identity management.<sup>138</sup>

Looking to the future, continued investment is needed not only in privacy topics ancillary to security, but also in automating privacy protection for the broadest aspects of use of data from all sources. Relevant topics include cryptography, privacy-preserving data mining (including analysis of streaming as well as stored) data,<sup>139</sup> formalization of privacy policies, tools for automating conformance of software to personal privacy policy and to legal policy, methods for auditing use in context and identifying violations of policy, and research on enhancing people's ability to make sense of the results of various big-data analyses. Development of technologies that support both quality analytics and privacy preservation on distributed data, such as secure multiparty computation, will become even more important, given the expectation that people will draw increasingly from

<sup>133</sup> *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology* (<http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd2013.pdf> [2012] and <http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf> [2010]).

<sup>134</sup> Federal Networking and Information Technology Research and Development Program, "Report on Privacy Research Within NITRD [Networking and Information Technology Research and Development], National Coordination Office for NITRD, April 23, 2014. [http://www.nitrd.gov/Pubs/Report\\_on\\_Privacy\\_Research\\_within\\_NITRD.pdf](http://www.nitrd.gov/Pubs/Report_on_Privacy_Research_within_NITRD.pdf)

<sup>135</sup> The Secure and Trustworthy Cyberspace program is the largest funder of relevant research. See: [http://www.nsf.gov/funding/pgm\\_summ.jsp?pins\\_id=504709](http://www.nsf.gov/funding/pgm_summ.jsp?pins_id=504709)

<sup>136</sup> In December 2013, the NSF directorates supporting computer and social science joined in soliciting proposals for privacy-related research. <http://www.nsf.gov/pubs/2014/nsf14021/nsf14021.jsp>.

<sup>137</sup> See: <http://www.iarpa.gov/index.php/research-programs/spar>

<sup>138</sup> NIST is responsible for advancing the National Strategy for Trusted Identities in Cyberspace (NSTIC), which is intended to facilitate secure transactions within and across public and private sectors. See: <http://www.nist.gov/nstic/>

<sup>139</sup> Pike, W.A. et al., "PNNL [Pacific Northwest National Laboratory] Response to OSTP Big Data RFI," March 2014.

data stored in multiple locations. The creation of tools that analyze the panoply of National, state, regional, and international rules and regulations for inconsistencies and differences will be helpful for the definition of new rules and regulations, as well as for those software developers that need to customize their services for different markets.

**Recommendation 4. OSTP, together with the appropriate educational institutions and professional societies, should encourage increased education and training opportunities concerning privacy protection, including professional career paths.**

Programs that provide education leading to privacy expertise (akin to what is being done for security expertise) are essential and need encouragement. One might envision careers for digital-privacy experts both on the software development side and on the technical management side. Employment opportunities should exist not only in industry (and government at all levels), where jobs focused on privacy (including but not limited to Chief Privacy Officers) have been growing, but also for consumer and citizen advocacy and support, perhaps offering “annual privacy checkups” for individuals. Just as education and training about cybersecurity has advanced over the past 20 years within the technical community, there is now opportunity to educate and train students about privacy implications and privacy enhancements, beyond the present small niche area occupied by this focus within computer science programs.<sup>140</sup> Privacy is also an important component of ethics education for technology professionals.

**Recommendation 5. The United States should take the lead both in the international arena and at home by adopting policies that stimulate the use of practical privacy-protecting technologies that exist today. This country can exhibit leadership both by its convening power (for instance, by promoting the creation and adoption of standards) and also by its own procurement practices (such as its own use of privacy-preserving cloud services).**

Section 4.5.2 described a set of privacy-enhancing best practices that already exist today in U.S. markets. PCAST is not aware of any more effective innovation or strategies being developed abroad; rather, some countries seem inclined to pursue what PCAST believes to be blind alleys. This circumstance offers an opportunity for U.S. technical leadership in privacy in the international arena, an opportunity that should be seized. Public policy can help to nurture the budding commercial potential of privacy-enhancing technologies, both through U.S. government procurement and through the larger policy framework that motivates private-sector technology engagement.

As it does for security, cloud computing offers positive new opportunities for privacy. By requiring privacy-enhancing services from cloud-service providers contracting with the U. S. government, the government should encourage those providers to make available sophisticated privacy enhancing technologies to small businesses and their customers, beyond what the small business might be able to do on its own.<sup>141</sup>

<sup>140</sup> A basis can be found in the newest version of the curriculum guidance of the Association for Computing Machinery (<http://www.acm.org/education/CS2013-final-report.pdf>). Given all of the pressures on curriculum, progress—as with cybersecurity—may hinge on growth in privacy-related research, business opportunities, and occupations.

<sup>141</sup> A beginning can be found in the Federal Government’s FedRAMP program for certifying cloud services. Initiated to address Federal agency security concerns, FedRAMP already builds in attention to privacy in the form of a required Privacy Threshold Analysis and in some situations a Privacy Impact Analysis. The office of the U.S. Chief Information Officer

#### 5.4 Final Remarks

Privacy is an important human value. The advance of technology both threatens personal privacy and provides opportunities to enhance its protection. The challenge for the U.S. Government and the larger community, both within this country and globally, is to understand what the nature of privacy is in the modern world and to find those technological, educational, and policy avenues that will preserve and protect it.

---

provides guidance on Federal uses of information technology that addresses privacy along with security (see <http://cloud.cio.gov/>). It provides specific guidance on the cloud and FedRAMP (<http://cloud.cio.gov/fedramp>), including privacy protection (<http://cloud.cio.gov/document/privacy-threshold-analysis-and-privacy-impact-assessment>).





## Appendix A. Additional Experts Providing Input

**Yochai Benkler**  
Harvard

**Eleanor Birrell**  
Cornell University

**Courtney Bowman**  
Palantir

**Christopher Clifton**  
Purdue University

**James Costa**  
Sandia National Laboratory

**Lorrie Faith Cranor**  
Carnegie Mellon University

**Deborah Estrin**  
Cornell NYC

**William W. (Terry) Fisher**  
Harvard Law School

**Stephanie Forrest**  
University of New Mexico

**Dan Geer**  
In-Q-Tel

**Deborah K. Gracio**  
Pacific Northwest National Laboratory

**Eric Grosse**  
Google

**Peter Guerra**  
Booz Allen

**Michael Jordan**  
University of California, Berkeley

**Philip Kegelmeyer**  
Sandia National Laboratory

**Angelos Keromytis**  
Columbia University

**Thomas Kalil**  
OSTP

**Jon Kleinberg**  
Cornell University

**Julia Lane**  
American Institutes for Research

**Carl Landwehr**  
George Washington University

**David Moon**  
Ernst & Young

**Keith Marzullo**  
National Science Foundation

**Martha Minow**  
Harvard Law School

**Tom Mitchell**  
Carnegie Mellon University



BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE

**Deirdre Mulligan**

University of California, Berkeley

**Leonard Napolitano**

Sandia National Laboratory

**Charles Nelson**

OSTP

**Chris Oehmen**

Pacific Northwest National Laboratory

**Alex “Sandy” Pentland**

Massachusetts Institute of Technology

**Rene Peralta**

National Institute of Standards and Technology

**Anthony Philippakis**

Genome Bridge

**Timothy Polk**

OSTP

**Fred B. Schneider**

Cornell University

**Greg Shipley**

In-Q-Tel

**Lauren Smith**

OSTP

**Francis Sullivan**

Institute for Defense Analysis

**Thomas Vagoun**

NITRD National Coordination Office

**Konrad Vesey**

Intelligence Advanced Research Activity

**James Waldo**

Harvard

**Peter Weinberger**

Google, Inc.

**Daniel J. Weitzner**

Massachusetts Institute of Technology

**Nicole Wong**

OSTP

**Jonathan Zittrain**

Harvard Law School

### Special Acknowledgment

PCAST is especially grateful for the rapid and comprehensive assistance provided by an ad hoc group of staff at the National Science Foundation (NSF), Computer and Information Science and Engineering Directorate. This team was led by Fen Zhao and Emily Grumbling, who were enlisted by Suzanne Iacono. Drs. Zhao and Grumbling worked tirelessly to review the technical literature, elicit perspectives and feedback from a range of NSF colleagues, and iterate on descriptions of numerous technologies relevant to big data and privacy and how those technologies were evolving.

#### NSF Technology Team Leaders

**Fen Zhao**, AAAS Fellow, CISE

**Emily Grumbling**, AAAS Fellow, Office of  
Cyberinfrastructure

#### Additional NSF Contributors

**Robert Chadduck**, Program Director

**Almadena Y. Chtchelkanova**, Program Director

**David Corman**, Program Director

**James Donlon**, Program Director

**Jeremy Epstein**, Program Director

**Joseph B. Lyles**, Program Director

**Dmitry Maslov**, Program Director

**Mimi McClure**, Associate Program Director

**Anita Nikolich**, Expert

**Amy Walton**, Program Director

**Ralph Wachter**, Program Director





President's Council of Advisors on Science and  
Technology (PCAST)

[www.whitehouse.gov/ostp/pcast](http://www.whitehouse.gov/ostp/pcast)

## NOTES

The White House, Interim Progress Report,  
Big Data: Seizing Opportunities, Preserving  
Values (February 2015)

Submitted by:  
Christin McMeley  
*Davis Wright Tremaine LLP*

Noga Rosenthal  
*Epsilon/Conversant*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



# BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES



## Interim Progress Report

February 2015

One year ago, President Obama spoke at the Department of Justice about changes in the technology we use for national security and signals intelligence purposes, and what those technological changes mean for privacy writ large. Recognizing that these technologies have implications beyond the national security arena, the President also called for a wide-ranging review of big data and privacy to explore how these technologies are changing our economy, our government, and our society, and to consider their implications for personal privacy. The goal of the review was to understand what is genuinely new and different about big data and to consider how best to encourage the potential of these technologies while minimizing risks to privacy, fair treatment, and other core American values.

Over the course of the 90-day inquiry, the big data and privacy working group—led by Counselor to the President John Podesta, Commerce Secretary Penny Pritzker, Energy Secretary Ernest Moniz, the President's science advisor Dr. John Holdren, and the President's economic advisor Jeff Zients—sought public input and engaged with academic researchers and privacy advocates, regulators and the technology industry, and advertisers and civil rights groups. The review was supported by a parallel effort by the President's Council of Advisors on Science and Technology (PCAST) to investigate the scientific and technological dimensions of big data and privacy.

The big data and privacy working group's report found that the declining cost of data collection, storage, and processing, coupled with new sources of data from sensors, cameras, and geospatial technologies, means that we live in a world where data collection is nearly



ubiquitous, where data retention can be functionally permanent, and where data analysis is increasingly conducted in speeds approaching real time. While there are promising technological means to better protect privacy in a big data world, the report's authors concluded these methods are far from perfect, and technology alone cannot protect privacy absent strong social norms and a responsive policy and legal framework. Finally, the report raised issues around other values potentially implicated by big data technology—particularly with regard to the potential for big data technologies to lead, purposely or inadvertently, to discriminatory outcomes on the basis of race, gender, socioeconomic status, or other categories.

But big data technologies continue to hold enormous promise, as the report identified—to streamline public services, to advance health care and education, and to combat fraud and complex crimes like human trafficking. A year after the President's request for this report, the Obama Administration has worked to advance a number of the concrete policy proposals offered in the report, both by launching new efforts and continuing to develop previously existing projects. The Administration continues to drive the national conversation, inside and outside of government, on how to maximize benefits while minimizing the risks and harms posed by a big data world.

## Key Recommendations

*The big data and privacy working group report identified six specific policy recommendations as deserving prompt action:*

- **Advance the Consumer Privacy Bill of Rights** because consumers deserve clear, understandable, reasonable standards for how their personal information is used in the big data era.
- **Pass National Data Breach Legislation** that provides for a single national data breach standard, along the lines of the Administration's 2011 Cybersecurity legislative proposal.
- **Extend Privacy Protections to non-U.S. Persons** because privacy is a worldwide value, and should be reflected in how the federal government handles personally identifiable information from non-U.S. citizens.
- **Ensure Data Collected on Students in School is used for Educational Purposes** to protect students from having their data shared or used inappropriately.
- **Expand Technical Expertise to Stop Discrimination** so that the federal government's lead civil rights and consumer protection agencies can identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes, and develop plans for investigating and resolving violations of law.
- **Amend the Electronic Communications Privacy Act** to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world—including by removing archaic distinctions between email left unread or over a certain age.

*The Administration is making significant progress on most of these recommendations:*

- The Department of Commerce solicited public comment on the Consumer Privacy Bill of Rights in light of new technologies, including those identified in the big data and privacy report, and the Obama Administration will release draft legislation in early 2015.
- President Obama released revised national data breach legislation, the Personal Data Notification & Protection Act, on January 12, 2015.
- Attorney General Eric Holder announced in June 2014 that the Administration would seek legislation extending to EU citizens the same right to judicial redress for intentional or willful wrongful disclosure of personal data exchanged under the U.S.-EU Data Protection and Privacy Agreement for law enforcement purposes, or for refusal to grant access or to rectify any errors in that information, as U.S. citizens would have under the Privacy Act of 1974. The Office of Management and Budget is working with departments and agencies to extend other privacy protections to non-U.S. citizens.
- President Obama announced the Student Digital Privacy Act, a national effort to ensure K-12 student data is used only for educational purposes, on January 12, 2015, in conjunction with new private sector commitments to help enhance privacy for students as well as a landmark voluntary effort by over 100 companies committing not to abuse education data.
- Several efforts have been undertaken to further the federal government's understanding of big data and discrimination, including studying the potential implications of using predictive analytics in law enforcement at the Department of Justice and by studying price discrimination at the Council of Economic Advisers. The White House Domestic Policy Council is preparing a follow-on report for release in early 2015 focusing on the potential of big data both to lead to discriminatory outcomes in key policy areas and to be used to counteract discrimination.

*Further progress on implementing the big data and privacy report's recommendations and related efforts is detailed in the following pages.*

## **1. Preserving Privacy Values**

The innovation driven by big data creates both tremendous opportunity and novel privacy challenges. The report explored privacy challenges across sectors, and suggested that we reexamine our conception of notice and consent, as well as the notion of use frameworks as a basis for managing privacy rights. The report suggested a number of specific steps forward in order to ensure that privacy protections evolve in a way that enables the social good that can result from big data, while protecting and empowering citizens.

### **Advance the Consumer Privacy Bill of Rights**

The report called on the Department of Commerce to advance the 2012 Consumer Privacy Bill of Rights by seeking public comment on big data developments and how they impact the CPBR's policies and then devise draft legislative text. This month, the Administration plans to release draft legislation based on public comments received during that comment period.

### **Pass National Data Breach Legislation**

The report called for the creation of a national data breach standard to benefit both consumers and businesses, in the face of a growing number of breaches and an inconsistent patchwork of state laws. In January 2015, President Obama announced the Personal Data Notification & Protection Act, a new legislative proposal to help bring peace of mind to all Americans, including the tens of millions whose personal and financial information has been compromised in a data breach. This proposal clarifies and strengthens the obligations companies have to notify customers when their personal information has been compromised, while providing companies with the certainty of a single, national standard—as well as criminalizing the illicit overseas trade in identities.

### **Bring Greater Transparency to the Data Services Industry**

In May, the Federal Trade Commission released an in-depth report on the data broker industry, concluding that data brokers operate with a fundamental lack of transparency. The Commission recommended that Congress consider enacting legislation to make data broker practices more visible to consumers and to give consumers greater control over the personal information collected and shared by data brokers.

### **Lead International Conversations on Big Data**

Data privacy has long been a component of the United States' bilateral and multilateral discussions. Well before the big data and privacy report, the Administration engaged in extensive consultation with data protection authorities, international civil society, and privacy experts from Europe and around the world.

Of particular note since the release of the report, high-ranking officials from the United States and Germany discussed the report's findings and bilateral cooperation on cyber issues as part of the third Cyber Bilateral Meeting in June 2014, including cybersecurity and critical infrastructure protection, cyber defense, combating cybercrime, Internet freedom, and Internet governance.

## Extend Privacy Protections to non-U.S. Persons

The report recommended that the OMB work with agencies to apply the Privacy Act to non-U.S. persons where practicable, or establish alternative privacy policies for personal data held by the federal government that provide appropriate and meaningful protections regardless of nationality. OMB has been leading an interagency process to implement this recommendation.

In addition to these general protections, the United States is actively pursuing efforts to grant certain rights of judicial redress to EU citizens and citizens of other nations that effectively share terrorism and law enforcement information with the United States and provide appropriate privacy protections. In the 2014 U.S.-EU Ministerial Meeting on Justice and Home Affairs, Attorney General Eric Holder made clear the United States' commitment to pursue this effort, and the Administration is working closely with members of Congress on this important measure.

## 2. Responsible Educational Innovation in the Digital Age

*"[D]ata collected on students in the classroom should only be used for educational purposes – to teach our children, not to market to our children. We want to prevent companies from selling student data to third parties for purposes other than education. We want to prevent any kind of profiling that puts certain students at a disadvantage as they go through school."*

- President Barack Obama at the Federal Trade Commission, January 12, 2015

Big data has the potential to transform education for the better, creating unprecedented educational opportunities—for instance, by tailoring lessons to a student's learning style, by opening up courses through online platforms, and by making it easier for parents, teachers, and students to identify where an individual student may be struggling and offer targeted instruction. These new technologies hold the potential to vastly improve student performance and to provide researchers with valuable insights about how students learn, which could help improve low-tech educational interventions as well. Beyond educational technology, the mere operation of schools produces vast amounts of data—data that can improve efficiency as well as education. However, the federal government must play its part to ensure that student data is not shared or used inappropriately. The Administration has taken significant steps to safeguard student data in the classroom and beyond, as well as promoting and enabling innovation in learning.

### Ensure Data Collected on Students in School is used for Educational Purposes

On January 12, 2015, the President proposed the Student Digital Privacy Act: a new legislative proposal designed to provide teachers and parents the confidence they need to enhance teaching and learning with the best technology—by ensuring that data collected in the educational context is used only for educational purposes. This bill, modeled on a landmark California statute, builds on the recommendations of the report, would prevent companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school—while still permitting important research initiatives to improve student learning outcomes, and efforts by companies to continuously improve the effectiveness of their learning technology products.

The legislation will be accompanied by new tools from the Department of Education to empower educators around the country. The Department of Education and its Privacy Technical Assurance Center play a critical role in protecting American children from invasions of privacy in the classroom. Alongside the President's call for legislation, he unveiled executive actions that will enhance that office's abilities to help ensure educational data is used in ways appropriate and in accordance with the educational mission—including a model terms of service and providing teacher training assistance.

The largest educational technology vendors also committed to help lead the way in ensuring the protection of students—and, as of today, over 100 of them have signed on to a pledge to provide important protections against misuse of students' data.

### **Recognize Digital Literacy as an Important 21st Century Skill**

Knowledge and efficient use of digital materials will become increasingly important as computer technologies begin to drive economic and educational empowerment. This recommendation was included in both the big data and privacy working group's recommendations and in the PCAST report. The Administration has advanced several initiatives that encourage digital literacy by connecting Americans to the latest technologies and strengthening the technical skills that can enable fluid use of the latest digital resources. These initiatives promote: (1) the literacy to help students be creators—not just consumers—with increased access to coding experiences, as the President illustrated by participating in the Hour of Code in fall 2014; (2) the literacy to be prepared to work in the STEM fields, through initiatives such as the President's Educate to Innovate campaign; (3) the literacy to use technology smartly, including empowering students to protect their privacy; and (4) literacy realized as access for all, including access to broadband at home and at school, an issue the President has tackled through the ConnectED Initiative. Connectivity is especially critical, as these initiatives must help bridge the digital divide and inequality of opportunity that often exists in educational contexts throughout the nation.

In the coming months, the White House will continue to work with stakeholders and other partners to develop new initiatives to make digital literacy opportunities more accessible and available for the American people.

## **3. Big Data and Discrimination**

One of the most notable findings of the big data and privacy report was that alongside its potential benefits to be used to increase access to credit or improve educational outcomes, there also exists the potential for big data technology to be used to discriminate against individuals, whether intentionally or inadvertently, potentially enabling discriminating outcomes, reducing opportunities and choices available to them.

As part of the national discussion prompted by the big data study, the civil rights community, industry and federal agencies began to identify possible principles and frameworks to guide uses of data. Before the report was completed, a coalition of civil rights organizations announced a set of civil rights principles for the big data era, focused on stopping high-tech profiling, ensuring fairness in automated decisions, preserving constitutional principles, enhancing individual control

of personal information, and protecting people from inaccurate data. The civil rights community worked with technologists and academics to organize an October 2014 conference on big data and discrimination and hopes to make it an annual event, with continuing strong participation from the federal government.

The White House considers this topic a priority, and is continuing to explore the implications of big data in this arena, including considering how big data technology can be used to shore up civil rights. Among other investments, the Obama Administration's budget for Fiscal Year 16 includes \$17 million for data science pilots at the National Science Foundation that seek to study issues around data interoperability; data policy and governance; and data security, privacy, integrity, and trustworthiness. These pilots will directly inform other federal big data research projects and will assist in developing the technological and policy expertise needed to tackle difficult problems like the potential for big data to lead to discriminatory outcomes.

#### **Pay Attention to the Potential for Big Data to Facilitate Discrimination**

The White House Domestic Policy Council and the Office of Science and Technology Policy will issue a follow-up report further exploring the implications of big data technologies for discrimination and civil rights. Specifically, the new report will take a deeper dive into how big data interacts with issues like employment and access to credit—considering both how the use of big data technologies can perpetuate discrimination and prevent it. The White House has engaged with leading researchers and advocates to develop recommendations on actions that can be taken to use big data to broaden opportunity and to prevent discrimination.

#### **Expand Technical Expertise to Stop Discrimination**

One of the key recommendations of the big data and privacy report was that the federal government's lead civil rights and consumer protection agencies should expand their technical expertise to be able to identify practices and outcomes facilitated by big data analytics that may have a discriminatory impact on protected classes, and develop a plan for investigating and resolving potential violations of law.

In June, the Office of Science and Technology Policy and the Georgetown University McCourt School of Public Policy's Massive Data Institute cohosted a fourth big data convening focused on the work of federal agencies. The multi-stakeholder workshop focused on federal agencies' use of open data and big data, best practices for sharing data within and between agencies and other partners, and how to address potential privacy and civil liberties concerns that arise from the use of big data.

In September, the Federal Trade Commission hosted a workshop entitled "Big Data: A Tool for Inclusion or Exclusion?" in its Washington offices. The workshop explored the use of big data and its impact on American consumers, with an eye towards low income and underserved consumers. The workshop highlighted concerns about whether big data may be used to categorize consumers in ways that may affect them unfairly, or even unlawfully.

#### **Deepen Understanding of Differential Pricing**

The White House Council of Economic Advisors conducted a study of commercial applications of

big data. The CEA explored whether companies will use the information they harvest to more effectively charge different prices to different customers. The economic literature on value-based price discrimination suggests that this will often, though not always, be welfare-enhancing for both businesses and consumers. However, individualized pricing based on estimates of cost or riskiness can raise concerns about fairness, particularly when consumers are unaware of the data or methods that companies employ. The CEA report finds that many companies already use big data for targeted marketing, and some are experimenting with personalized pricing, though examples of personalized pricing remain fairly limited.

#### **4. Law Enforcement and Security**

Big data can be used to make our communities safer and strengthen our national security, but raises equally important questions for our personal privacy and civil liberties. The big data and privacy report encouraged our national security, homeland security, law enforcement, and intelligence communities to vigorously experiment with and employ lawful big data technology while adhering to full accountability, oversight, and relevant privacy requirements.

##### **Review Law Enforcement's Use of Predictive Analytics**

In light of the report, the Department of Justice recently conducted a review of the current use of predictive analytics in law enforcement. This review focused on the DOJ's own use of analytic tools, as well as on some of the programs the Department helps fund through research grants. DOJ also reviewed some of the newer technologies in use by state and local law enforcement agencies.

DOJ concluded that new data-driven technologies have the potential to bring significant benefits to our criminal justice system. Many of these technologies build on traditional techniques and are designed to help law enforcement agencies allocate scarce resources more efficiently to prevent crime. The Department also observed that the use of predictive analytics raises issues and potential challenges that are worthy of continued attention, so that predictive techniques continue to be driven by the core enforcement goals of protecting the public and ensuring fairness in our justice system.

Going forward, DOJ will work collaboratively with stakeholders and develop guidance for the use of predictive analytics by state and local law enforcement agencies. The Department will also continue to engage in ongoing conversations about the effectiveness and impact of new predictive techniques.

##### **Foster Responsible Use and Privacy Best Practices with State and Local Law Enforcement Entities Receiving Federal Grants**

The big data and privacy report recommended that that federal agencies with expertise in privacy and data practices provide technical assistance to state, local, and other federal law enforcement agencies seeking to deploy big data techniques. In November 2014, DOJ developed a supplemental guide to augment its privacy-related technical assistance library for state, local, and tribal law enforcement agencies, entitled *Resource Guide for Enhancing Community*

*Relationships and Protecting Privacy and Constitutional Rights.* This supplemental guide serves as a point of reference for state, local, and tribal law enforcement entities in fostering the development of responsible privacy practices. Additionally, DOJ continues to engage in outreach to state, local, and tribal law enforcement entities through participation in trainings and conferences on related issues.

#### **Review Government Use of Commercial Databases**

The report recommended that the federal government review uses of commercially available databases on U.S. citizens, focusing on use of services that employ big data techniques and ensuring that they incorporate appropriate oversight and protections for privacy and civil liberties. DOJ and the Office of the Director of National Intelligence, together with the Office of Management and Budget, are leading an effort to review the use of commercial databases by the federal government. In particular, they are examining the use of commercial databases by federal agencies in the context of public administration, law enforcement, and national security. The review process will include recommendations for how the government can use the databases while also protecting privacy and civil liberties.

#### **Implement Best Practices for Controlled Use and Storage of Data at Agencies**

Efforts are underway on several fronts to maximize privacy protections by improving agency use and storage of data, and to strengthen cybersecurity in general. For instance, the Department of Homeland Security is working across government and the private sector to identify and leverage the opportunities big data analytics presents to strengthen cybersecurity. This will include coordinating the development or changes of necessary policies to ensure that data is appropriately protected and secured.

The Office of Management and Budget is leading an effort to expand successful data management and security pilots across government and has connected practitioners and leaders from innovative and effective data management initiatives at several federal agencies to foster an exchange of success stories and lessons learned.

The National Security Council is asking the President's National Security Telecommunications Advisory Committee to undertake a private sector-led study with recommendations on using big data analytics to strengthen cybersecurity.

The Administration has also continued to address the challenges to information sharing. The Department of Justice and the Federal Trade Commission issued guidance that sharing of cyber threat information should not raise anti-trust concerns—thus addressing a long-standing concern from industry. The Department of Homeland Security is modernizing its Protected Critical Infrastructure Information program to enable its use for the protection of private sector information voluntarily submitted to the Department for the purposes of improving network defenses.

#### **Advance Cybersecurity and Consumer Protection with 2015 Summit**

On February 13, 2015, the White House will host a cybersecurity and consumer protection summit at Stanford University. The summit will bring together major stakeholders on cybersecurity and consumer financial protection issues from the public and private sectors to discuss a range of



topics, including creating improved cybersecurity practices and strengthening cyber threat information sharing. The summit will also serve as the next step in the President's BuySecure Initiative, will help advance national efforts the government has led on consumer financial protection and critical infrastructure cybersecurity, and will build on efforts to improve cybersecurity at a wide range of companies.

## 5. Data as a Public Resource

The report urged agencies across government to consider data as a national, public resource, and make it broadly available to the public wherever possible. This effort continues the Obama Administration's commitment to open data and open government from the first day of this Administration. To date, there are over 134,000 datasets available on [Data.gov](https://data.gov) for public use. The Administration has made great strides towards bringing technologists into government through the creation of the United States Digital Service, 18F, and the Presidential Innovation Fellowship to ensure that the government continues to meet the needs of Americans who expect the high quality digital content, as well as make data open and usable to the public.

### Continue Making Government Data Available to the Public

The Administration has launched a series of Open Data Initiatives that have unleashed large volumes of valuable data in areas such as health, energy, education, public safety, finance, and global development. For example, the Climate Data Initiative, launched in March 2014, leverages open climate data to fuel innovation and private sector entrepreneurship to advance climate change preparedness and community resilience through the development of data products, tools, and applications that are geared toward solving real-life challenges.

This Administration is committed to making open and machine-readable data the default for government information. Federal agencies have continued to increase the quantity and quality of open data over the past year. Each quarter, federal agencies add additional datasets to their Public Data Listings. [Data.gov](https://data.gov) automatically updates its inventory by harvesting the Public Data Listings each day. Nearly every agency has data listed on [Data.gov](https://data.gov).

### Adopting Open Data Best Practices

Many federal agencies have adopted new open data processes to better manage their data at an organizational level. For example, over the past year, NASA has continued to develop an agency-level NASA Information Architecture Management (NIAM) process to share and reuse data from across agency components. Through the NIAM process, NASA significantly improved its common metadata, contract language, and search capacity, and as a result, NASA increased its Enterprise Data Inventory from 25 datasets to more than 3,800 datasets between November 2013 and November 2014.

Increased customer engagement is helping to improve the federal open data policy. For example, agencies have learned that one of the most common complaints of data users is the use of PDF—rather than machine-readable—formats. OMB and OSTP are now working with agencies to reduce the number of PDFs and make machine-readability the standard for all government data.

## Issues Needing Further Attention

Some efforts await Congressional or stakeholder action. For instance, efforts on Capitol Hill to amend the almost 30-year-old Electronic Communications Privacy Act have seen little progress since the report was issued. The report recommended that Congress amend ECPA to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world—including by removing archaic distinctions between email left unread or over a certain age.

In 2012, the Administration expressed support for the multistakeholder development of a Do Not Track standard that could be used by consumers regardless of browser preference or operating system. This was a novel multi-stakeholder effort, bringing together the technical community, advertisers, publishers, and privacy experts, and the big data and privacy working group called for the initiative to continue its efforts. Disappointingly—and despite no downturn in consumer interest—there have been delays in moving this initiative forward. Stakeholders should recommit to developing new voluntary tools, including Do Not Track, to safeguard users' privacy.

## Conclusion

Less than a year after the release of the big data and privacy working group's findings, the Obama Administration has made significant progress in furthering the majority of the recommendations made in the big data and privacy report. Policy development remains actively underway on complex recommendations, including extending more privacy protections to non-U.S. persons and scaling best practices in data management across government agencies. And in big data and discrimination, the civil rights and privacy communities will continue to play an active and critical role in driving the conversation, partnering with the federal government, and surfacing new issues for consideration in this new field.

Beyond the conclusions of the big data and privacy working group, the insights in the report have also had influence on Administration policy. In his State of the Union address, President Obama announced an ambitious plan to advance understanding of precision medicine, an emerging field that holds the promise of revolutionizing how we improve health and treat disease. Leveraging advances in genomics, clinical practice, big data technology, and other fields, the Precision Medicine Initiative will seek to create a one-million-strong national research cohort and to accelerate discovery of tailored treatments for cancers. Data security and patient privacy will be paramount to the Precision Medicine Initiative. The effort will incorporate the lessons learned by other federal agencies and the issues identified in the big data and privacy report and solicit input from a diverse range of privacy stakeholders from the earliest days in order to integrate rigorous privacy protections throughout the program.

The big data and privacy working group concluded that, despite the newness of the field, big data is already saving lives, making the economy and the government work better, and saving taxpayer dollars along the way. Big data will continue to contribute to and shape our society, and the Obama Administration will continue working to ensure that government and civil society strive to harness the power of these technologies while protecting privacy and preventing harmful outcomes.

## NOTES

Julie Brill, Commissioner, U.S. Federal  
Trade Commission, Speech, Keynote  
Address Before the 23rd Computers Freedom  
and Privacy Conference (June 26, 2013)

Submitted by:  
Noga Rosenthal  
*Epsilon/Conversant*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



Reclaim Your Name  
23<sup>rd</sup> Computers Freedom and Privacy Conference  
Keynote Address by  
Commissioner Julie Brill  
Federal Trade Commission  
Washington, DC  
June 26, 2013

Thank you for that generous introduction and for allowing me the opportunity to speak to you. Today I'd like to address big data and the challenges it presents for consumers, for markets, and for agencies like the FTC tasked with safeguarding both. The topic is timely. This month, Edward Snowden, a former employee of a national security contractor, gave the world a crash course in just how much privacy we can expect if we participate at all in an increasingly online and mobile marketplace. He leaked details of some of the National Security Administration's data collection efforts, one program that collects telephone metadata from US telephone companies and another that monitors international Internet and email traffic.

We don't have to pass judgment on the NSA or Snowden to acknowledge the disclosures have sparked a necessary and overdue debate on how to balance national security against citizens' privacy rights. For those of us who have been looking at the issue of privacy in the Internet age for several years, there is a further benefit: Americans are now more aware than ever of how much their personal data is free-floating in cyberspace, ripe for any data miner – government or otherwise – to collect, use, package, and sell.

Many consumers have been loath to examine too closely the price we pay, in terms of forfeiting control of our personal data, for all the convenience, communication, and fun of a free-ranging and mostly free cyberspace. We are vaguely aware that cookies attach to us wherever we go, tracking our every click and view. We tell Trip Advisor our travel plans, open our calendars to Google Now, and post our birthdays on Facebook. We broadcast pictures of our newborns on Instagram; ask questions about intimate medical conditions on WebMD; and inform diet sites what we ate that day and how long we spent at the gym. Google Maps, Twitter and Four Square know where we are. Uber, Capital BikeShare, and Metro's trip planner know where we're going and how we plan to get there.

We spew data every minute we walk the street, park our cars, or enter a building – the ubiquitous CCTV and security cameras blinking prettily in the background – every time we go online, use a mobile device, or hand a credit card to a merchant who is online or on mobile. We spend most of our days, and a good deal of our nights, surfing the web, tapping at apps, or powering on our smart phones, constantly adding to the already bursting veins from which data miners are pulling pure gold. That's where the "big" in "big data" comes from.

We send our digital information out into cyberspace and get back access to the magic of our wired lives. We sense this, but it took Snowden to make concrete what exactly the exchange means – that firms or governments or individuals, without our knowledge or consent, and often in surprising ways, may amass private information about us to use in a manner we don’t expect or understand and to which we have not explicitly agreed.

It is disconcerting to face how much of our privacy we have already forfeited. But with that knowledge comes power – the power to review, this time with eyes wide open, what privacy means – or should mean – in the age of the Internet. I believe that’s what President Obama meant last week when he called for a “national conversation...about the general problem of these big data sets because this is not going to be restricted to government entities.”

I’d like to pose two questions that are key to getting this conversation going, and then spend some time today trying to answer them. First, what are the major challenges to privacy posed by big data, particularly in its use in the commercial arena? And second, what steps can we take to meet these challenges?

But before I start, I want to make clear that big data is not synonymous with the evil empire. Most of us, myself included, rely on and enjoy our phones, apps, emails, and other programs that collect, store, and analyze large stocks of raw data. In their book, *Big Data*<sup>1</sup>, Victor Mayer-Schonberger and Ken Cukier cite numerous examples of how big data benefits us every day: spam filters adapt as junk email changes; dating sites pair couples based on attributes that correlate to previous successful matches; cars brake before we sense danger; online bookstores tell us what we will want to read next.

And these benefit go beyond making sure we don’t receive announcements of bogus lottery winnings or suffer through too many awkward blind dates – though I have single friends who tell me the latter innovation is Nobel Prize quality stuff. Big data is already revolutionizing health care. Mayer-Schonberger and Cukier write of Google, in 2009, analyzing the correlation between relevant user searches, such as “medicines for cough and cold,” and reported flu outbreaks from past years, to predict where – down to the region and state – H1N1 would strike. Another more recent example is the research project dubbed “Artemis” underway at Toronto’s Hospital for Sick Children. Doctors there are collecting and analyzing second-by-second vital statistics for premature newborns. They hope the resulting big database will allow clinicians to spot the onset of infection – a serious threat to these infants – in time to treat it effectively or ward it off altogether.

The financial world has long employed big data. Actuaries were using demographics and other trends to set life and auto insurance rates long before insurance salesman Fred MacMurray tried to help his paramour Barbara Stanwyck beat the number crunchers to get a big payout in the 1944 film *Double Indemnity*. By the 1960s, with the

---

<sup>1</sup> VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK*, 11 (2013) (hereinafter *Big Data*).

advent of modern credit reporting agencies and their files on millions of Americans, consumers could access credit without knowing their bankers, thus greasing the wheels of the growing economy. But with the credit reporting agencies' large databases came errors and unease about the amount of information – and hence power – these agencies held, due to their new-found ability to draw inferences and correlations that were not possible a decade earlier. As a result, in 1970, Congress passed the Fair Credit Reporting Act,<sup>2</sup> which contains rules about how credit reporting agencies and their customers can use the information and inferences drawn from these large databases.

Fast forward to today. We are awash in data. Estimates are that 1.8 trillion gigabytes of data were created in the year 2011 alone – that's the equivalent of every U.S. citizen writing 3 tweets per minute for almost 27,000 years.<sup>3</sup> Ninety percent of the world's data, from the beginning of time until now, has been generated over the past two years,<sup>4</sup> and it is estimated that that total will double every two years from now on.<sup>5</sup> As the costs of storing data plummet and massive computing power becomes widely available, crunching large data sets is no longer the sole purview of gigantic companies or research labs. As Schonberger-Mayer and Cukier write, big data has become democratized.

#### First Challenge: the Fair Credit Reporting Act

This astounding spread of big data gives birth to its first big challenge: how to educate the growing and highly decentralized community of big data purveyors about the rules already in place governing the ways certain kinds of data can be used. For instance, under the Fair Credit Reporting Act, or "FCRA," entities collecting information across multiple sources and providing it to those making employment, credit, insurance and housing decisions must do so in a manner that ensures the information is as accurate as possible and used for appropriate purposes.

The Federal Trade Commission has warned marketers of mobile background and criminal screening apps that their products and services may come under the FCRA, requiring them to give consumers notice, access, and correction rights.<sup>6</sup> We've also

---

<sup>2</sup> Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970).

<sup>3</sup> Lucas Mearian, *World's data will grow by 50X in next decade, IDC study predicts*, COMPUTERWORLD, June 28, 2011, available at [http://www.computerworld.com/s/article/9217988/World\\_s\\_data\\_will\\_grow\\_by\\_50X\\_in\\_next\\_decade\\_IDC\\_study\\_predicts?pageNumber=1](http://www.computerworld.com/s/article/9217988/World_s_data_will_grow_by_50X_in_next_decade_IDC_study_predicts?pageNumber=1).

<sup>4</sup> *Big Data, for Better or Worse: 90% of World's Data Generated over Last Two Years*, SCIENCE DAILY, May 22, 2013, available at <http://www.sciencedaily.com/releases/2013/05/130522085217.htm>.

<sup>5</sup> Steve Lohr, *The Age of Big Data*, N.Y. Times, February 11, 2012, available at <http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&r=0>.

<sup>6</sup> See Press Release, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), available at <http://www.ftc.gov/opa/2012/02/mobileapps.shtm>. The FTC has issued similar warning letters to app developers and data brokers that appeared to be selling consumer information for use in tenant screening, and in making insurance and employment decisions and firm offers of credit: See Press



entered into consent decrees that allow us to monitor the activities of other apps and online services that have similarly wandered into FCRA territory.<sup>7</sup> But while we are working hard to educate online service providers and app developers about the rules surrounding collecting and using information for employment, credit, housing, and insurance decisions, it is difficult to reach all of those who may be – perhaps unwittingly – engaged in activities that fall into this category.

Further, there are those who are collecting and using information in ways that fall right on —or just beyond —the boundaries of FCRA and other laws. Take for example the new-fangled lending institutions that forgo traditional credit reports in favor of their own big-data-driven analyses culled from social networks and other online sources.<sup>8</sup> Or eBureau, which prepares rankings of potential customers that look like credit scores on steroids. The New York Times describes this company as analyzing disparate data points, from “occupation, salary and home value to spending on luxury goods or pet food, ... with algorithms that their creators say accurately predict spending.”<sup>9</sup> These “e-scores” are marketed to businesses, which use them to decide to whom they will offer their goods and services and on what terms. It can be argued that e-scores don’t yet fall under FCRA because they are used for marketing and not for determinations on ultimate eligibility. But what happens if lenders and other financial service providers do away with their phone banks and storefronts and market their loans and other financial products largely or entirely online? Then, the only offers consumers will see may be those tailored based on their e-scores. Without FCRA protections, a consumer would not know if her e-score led to a higher loan rate or insurance premium, nor would she be able to access and correct any erroneous information about her.

Another class of decisions increasingly based on big data – what the FTC has called “eligibility” determinations – can also – if founded on inaccurate information – do real harm to consumers.<sup>10</sup> These include determinations about whether a consumer is too risky to do business with, engaged in fraud, or ineligible to enroll in certain clubs, dating

---

Releases, e.g., FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), *available at* <http://www.ftc.gov/opa/2013/05/databroker.shtm>, and FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act (Apr. 3, 2013), *available at* <http://www.ftc.gov/opa/2013/04/tenant.shtm>.

<sup>7</sup> See Press Release, Marketers of Criminal Background Screening Reports To Settle FTC Charges They Violated Fair Credit Reporting Act (Jan. 10, 2013), *available at* <http://www.ftc.gov/opa/2013/01/filiquarian.shtm>.

<sup>8</sup> Evelyn M. Rusli, *Bad Credit? Start Tweeting*, WALL ST. J., Apr. 1, 2013, *available at* <http://online.wsj.com/article/SB10001424127887324883604578396852612756398.html>.

<sup>9</sup> Natasha Singer, *Secret E-Scores Chart Consumers’ Buying Power*, N.Y. TIMES, Aug. 18, 2012, *available at* <http://www.nytimes.com/2012/08/19/business/electronic-scores-rank-consumers-by-potential-value.html?pagewanted=all>.

<sup>10</sup> FED. TRADE COMM’N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) (hereinafter 2012 Privacy Report) at 68–70, *available at* <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

services, schools, or other programs. Though any of these decisions could deeply affect consumers, the data used to make them may not fall within the confines of the FCRA.

The FCRA is a law that establishes the fair and prudent use of certain types of consumer data, and it is a law that is both relevant and worth preserving. But our big data world strains the seams of the FCRA. Our challenge is to figure out how FCRA's principles can coexist with new ways of collecting and using information – how consumers can maintain notice, access, and correction rights on all the dossiers – not just credit reports – that inform important decisions on eligibility as well as offers in areas such as housing, employment, finances, and insurance.

### Second Challenge: Transparency

The second big challenge to big data is transparency. Consumers don't know much about either the more traditional credit reporting agencies and data brokers or the newer entrants into the big data space. In fact, most consumers have no idea who is engaged in big data predictive analysis.

To their credit, some data brokers allow consumers to access some of the information in their dossiers, approve their use for marketing purposes, and correct the information for eligibility determinations.<sup>11</sup> In the past, however, even well-educated consumers have had difficulty obtaining meaningful information about what the data brokers know about them.<sup>12</sup> Just yesterday, “the big daddy of all data brokers”, Acxiom, announced that it plans to open its dossiers so that consumers can see the information the company holds about them.<sup>13</sup> This is a welcome step. But since most consumers have no way of knowing who these data brokers are, let alone finding the tools the companies provide, the reality is that current access and correction rights provide only the illusion of transparency.

### Third Challenge: Notice and Choice

A third challenge involves those aspects of big data to which the FCRA is irrelevant – circumstances in which data is collected and used for determinations unrelated to credit, employment, housing, and insurance, or other eligibility decisions. We need to consider these cases within the frameworks of the Federal Trade Commission

---

<sup>11</sup> See, e.g., ACXIOM, available at <http://www.acxiom.com/site-assets/privacy-acxiom-marketing-products/> (last visited June 24, 2013); EPSILON, available at <http://www.epsilon.com/consumer-info/consumer-guide-direct-marketing> (last visited June 24, 2013); and eBUREAU, available at <http://www.ebureau.com/privacy-center> (last visited June 24, 2013).

<sup>12</sup> Natasha Singer, *Consumer Data, but Not for Consumers*, N.Y. TIMES, Aug. 18, 2012, available at [http://www.nytimes.com/2012/07/22/business/acxiom-consumer-data-often-unavailable-to-consumers.html?pagewanted=all&\\_r=1&\\_](http://www.nytimes.com/2012/07/22/business/acxiom-consumer-data-often-unavailable-to-consumers.html?pagewanted=all&_r=1&_).

<sup>13</sup> Adam Tanner, *Finally You'll Get to See the Secret Consumer Dossier They Have On You*, FORBES, June 25, 2013, available at <http://www.forbes.com/sites/adamtanner/2013/06/25/finally-youll-get-to-see-the-secret-consumer-dossier-they-have-on-you/>.

Act, the OECD's Fair Information Privacy Principles,<sup>14</sup> and the FTC's 2012 Privacy Report,<sup>15</sup> for it is within those contexts we can see how big data is testing established privacy principles such as notice and choice.

One comparison highlights the difficulties of providing notice and consent in the context of big data – that of Artemis, the Toronto research project on infections in premature newborns, and the well-known, even infamous, example of the department store Target's big-data-driven campaign to identify pregnant customers. Over a year ago, the New York Times reported on Target's efforts to develop, through analysis of consumers' purchases at its stores, a "pregnancy prediction" score.<sup>16</sup> Target was able to calculate, not only whether a consumer was pregnant, but also when her baby was due. It used the information to win the consumer's loyalty by offering coupons tailored to her stage of pregnancy.

Obviously, Artemis and Target use big data for different ends: saving the lives of premature infants versus selling more maternity clothes and bassinets. There's no value judgment in that statement: Medical researchers look to improve our health; department stores seek to sell us stuff. We all want infant mortality to decline, and we all need a place to go to buy inexpensive baby clothes and diapers. The important point here is that, because of the context of the different relationships at issue, Artemis's use of Big Data allows for meaningful notice and choice within an appropriate regulatory regime, whereas Target did not – could not – provide meaningful notice and choice about its pregnancy predictor score project.

Artemis and other quality research projects inform parents of the data they are collecting from the babies and receive consent to do so.<sup>17</sup> Indeed, collecting information about their premature infants in order to provide better care is a critical part of the context of the relationship between the parents and the hospital.

Target's research and where it lands within the context of the retailer's relationship with the consumer is quite different. Let's assume Target didn't use any health information in creating its pregnancy predictor score, but instead tracked buying

---

<sup>14</sup> Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, (Sept. 23, 1980) available at <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm>.

<sup>15</sup> 2012 Privacy Report, *supra* note 10.

<sup>16</sup> Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, available at <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all>.

<sup>17</sup> In the United States, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d-9, requires hospitals, doctors, health insurance companies and their business partners are required to follow strict guidelines on how they handle health information about patients and insureds. And Institutional Review Boards ensure that human research is conducted ethically, including by maintaining the privacy of research subjects. See Institutional Review Board Guide Book at Chapter 3, [http://www.hhs.gov/ohrp/archive/irb/irb\\_guidebook.htm](http://www.hhs.gov/ohrp/archive/irb/irb_guidebook.htm).

patterns such as the purchase of prenatal vitamins and lotions with the subsequent purchase of newborn-size diapers. Given the context of the consumer's retail relationship with the store, I believe it would be impossible for Target to ask the consumer in a meaningfully way to consent to participating in the market study. The whole point of Target's big data project – indeed the point of many such big data projects – is to take innocuous information – here purchases at a store – and create an algorithm that makes sensitive predictions – here, whether a customer is pregnant.

To be clear, I don't have any information indicating that Target sold its pregnancy predictor score or lists of pregnant customers to third parties. Yet we can easily imagine a company that could develop algorithms that will predict other health conditions – diabetes, cancer, mental illness – based on information about routine transactions – store purchases, web searches, and social media posts – and sells that information to marketers and others.

And actually, you don't have to imagine it; it is already happening. The Financial Times recently highlighted how some data brokers collect personal details so intimate it makes Target's efforts seem almost quaint. One firm, [LeadsPlease.com](http://LeadsPlease.com), reportedly sells the names, mailing addresses, and medication lists of people with diseases like cancer or clinical depression. Another data broker, ALC Data, reportedly offers lists of consumers, their credit scores, and their specific ailments.<sup>18</sup>

Undoubtedly Target (and other companies in a similar position) provides some notice about how it collects and uses information to its *online* shoppers. But there is nothing in the context of a retail purchase that implies notice and consent – nothing that reasonably informs the consumer her data might be collected to make predictions about sensitive health conditions or seeks her consent to do so. And if the store were to try to make the notice and consent explicit? Imagine walking into Target and reading a sign on the wall or a disclosure on a receipt that says: "We will analyze your purchases to predict what health conditions you have so that we can provide you with discounts and coupons you may want." That clear statement would surprise – and alarm – most of us.

Big data advocates will point out that the FCRA delineates the inappropriate uses of sensitive data like health status. If data brokers aren't employing their health projections for one of these forbidden uses, then what is the harm? In fact, these advocates will say that predictive information about health conditions could help consumers reduce their risk of disease or control their symptoms, an end result that more than balances any breach of privacy.

The argument is compelling. But when health information flows outside the protected HIPAA environment, I worry about three things. First, as I mentioned before, how sensitive health information might be used to make decisions about eligibility that fall outside the contours of the FCRA, without notice or choice to the consumer. Second,

---

<sup>18</sup> Emily Steel, *Companies scramble for consumer data*, FINANCIAL TIMES, June 12, 2013, available at <http://www.ft.com/intl/cms/s/0/f0b6edc0-d342-11e2-b3ff-00144feab7de.html#axzz2XEcg1Gh>.

what will happen if this sensitive health information falls into the wrong hands through a data security breach – more on that in a minute. And third, what damage is done to our individual sense of privacy and autonomy in a society in which information about some of the most sensitive aspects of our lives is available for analysts to examine without our knowledge or consent, and for anyone to buy if they are willing to pay the going price.

#### Fourth Challenge: Deidentification

The final big challenge of big data that I would like to discuss is one that I've been assured by many of its proponents I shouldn't strain too hard to solve – that of predictive analytics attaching its findings to individuals. Most data brokers and advertisers will tell you they are working with de-identified information, that is, data stripped of a name and address. And that would be great if we didn't live in a world where more people know us by our user names than our given ones. Our online tracks are tied to a specific smartphone or laptop through UDIDs, IP addresses, "fingerprinting" and other means. Given how closely our smartphones and laptops are associated with each of us, information linked to specific devices is, for all intents and purposes, linked to individuals.

Furthermore, every day we hear how easy it is to reattach identity to data that has been supposedly scrubbed. In an analysis just published in *Scientific Reports*, researchers found that they could recognize a specific individual with 95 percent accuracy by looking at only four points of so-called "mobility data" tracked by recording the pings cell phones send to towers when we make calls or send texts.<sup>19</sup> NSF-funded research by Alessandro Acquisti has shown that, using publicly available online data and off-the-shelf facial recognition technology, it is possible to predict – with an alarming level of accuracy – identifying information as private as an individual's social security number from an anonymous snapshot.<sup>20</sup>

Target was most certainly linking its pregnancy forecasts with individuals' names, street addresses, and maybe phone numbers, email and IP addresses. How else could the retailer deliver the targeted coupon offers? And we know nothing about how long Target planned to hold onto this health information, and in what form it would be held.

We are all very familiar with the harms that can occur when there is a data breach. The risk of those injuries is multiplied ten-fold by big data's need to collect and store vast amounts of linkable data. The very way big data works – churning through personal details collected and saved without a specific purpose or expiration date – flies in the face of data minimization, one of the main fair information principles embedded in "privacy by design". Reducing the real damage data breaches can cause is one reason the FTC is urging big data users to commit to a robust program to de-identify their information.

---

<sup>19</sup> Yves-Alexandre de Montjoye, et. al., *Unique in the Crowd: The privacy bounds of human mobility*, 3 *SCI REP.* 1376 (2013).

<sup>20</sup> ALESSANDRO ACQUISTI, et. al., HEINZ COLLEGE & CYLAB CARNEGIE MELLON UNIVERSITY, *FACES OF FACEBOOK: PRIVACY IN THE AGE OF AUGMENTED REALITY*, (draft version) (2011), available at <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf>.

Clearly, simply deleting the name and address columns from big databases is not enough to keep anonymous the private information collected from consumers. The FTC has called on companies trafficking in big data to take both technological and behavioral steps to make sure the information they use in their advertising is truly and completely de-identified. They should do everything technically possible to strip their data of identifying markers; they should make a public commitment not to try to re-identify the data; and they should contractually prohibit downstream recipients from doing the same.<sup>21</sup>

How would this work in practice? Say Des Moines, Iowa wants to solve its terrible rush hour traffic congestion problems. City planners believe that the most useful information to help them tackle the problem is cellphone data, because cell phones are always on, and the data from them uniquely depicts traffic patterns and bottlenecks. Of course, Verizon and Sprint could not just hand over their customer's cell phone data, because – in the FTC's view – geolocation information linked to an individual is classic sensitive personal data. But the carriers could, as best as possible, scrub the data of sensitive personal information, and then – before they hand it over or allow Des Moines to use it – require Des Moines to sign a contract that specifically prohibits any effort to re-identify the data in any way, or to provide it to other parties.

Robust deidentification efforts along these lines will solve some of the problem. But because much of big data is created through predictive analysis, and because much of the analytics are for the purpose of gaining insights into specific individuals, chunks of big data will always be, by their very nature, identifiable or linkable to individuals.

#### Solutions to Notice, Choice and Transparency

So let's turn to some ways to solve the challenges big data poses to meaningful notice and choice as well as transparency. A part of the solution will be for companies to build more privacy protections into their products and services, what we at the FTC call "privacy by design". We have recommended that companies engage in cradle-to-grave review of consumer data as it flows through their servers, perform risk assessments, and minimize and deidentify data wherever possible.<sup>22</sup> Mayer-Schonberger and Cukier have helpfully called for the creation of "algorithmists" – licensed professionals with ethical responsibilities for an organization's appropriate handling of consumer data.<sup>23</sup> But the algorithmist will only thrive in an environment that thoroughly embraces "privacy by design," from the C-suite to the engineers to the programmers.

And unfortunately, even if the private sector embraces privacy by design and we license a cadre of algorithmists, we will not have met the fundamental challenge of big

---

<sup>21</sup> 2012 Privacy Report, *supra* note 10, at 21.

<sup>22</sup> *Id.* at 22.

<sup>23</sup> Big Data, *supra* note 1, at 180 – 182.

data in the marketplace: that is, consumers' loss of control of their most private and sensitive information.

Changing the law would help. I support legislation that would require data brokers to provide notice, access, and correction rights to consumers scaled to the sensitivity and use of the data at issue. For example, Congress should require data brokers to give consumers the ability to access their information and correct it when it is used for eligibility determinations, and the ability to opt-out of information used for marketing.

But we can begin to address consumers' loss of control over their most private and sensitive information even before legislation is enacted. I would suggest we need a comprehensive initiative – one I am calling “Reclaim Your Name.” Reclaim Your Name would give consumers the knowledge and the technological tools to reassert some control over their personal data – to be the ones to decide how much to share, with whom, and for what purpose – to reclaim their names.

Reclaim Your Name would empower the consumer to find out how brokers are collecting and using data; give her access to information that data brokers have amassed about her; allow her to opt-out if she learns a data broker is selling her information for marketing purposes; and provide her the opportunity to correct errors in information used for substantive decisions – like credit, insurance, employment, and other benefits.

Over a year ago, I called on the data broker industry to develop a user-friendly, one-stop online shop to achieve these goals. Over the past several months, I have discussed the proposal with a few leaders in the data broker business, and they have expressed some interest in pursuing ideas to achieve greater transparency. I sincerely hope the entire industry will come to the table to help consumers reclaim their names.

In addition, data brokers that participate in Reclaim Your Name would agree to tailor their data handling and notice and choice tools to the sensitivity of the information at issue. As the data they handle or create becomes more sensitive – relating to health conditions, sexual orientation, and financial condition – the data brokers would provide greater transparency and more robust notice and choice to consumers.

The credit reporting industry has to do its part, too. There are simply too many errors in traditional credit reports.<sup>24</sup> The credit bureaus need to develop better tools to help consumers more easily obtain and understand their credit reports so they can correct them. I have asked major credit reporting agencies to improve and streamline consumers' ability to correct information across multiple credit reporting agencies.

---

<sup>24</sup> See Press Release, In FTC Study, Five Percent of Consumers Had Errors on Their Credit Reports That Could Result in Less Favorable Terms for Loans (Feb. 11, 2013), available at <http://www.ftc.gov/opa/2013/02/creditreport.shtm>. The report revealed that one in twenty US consumers (10 million people) had errors in their credit report that could result in less favorable terms for credit.

I will continue to work on the contours of Reclaim Your Name over the next several months. I look forward to discussing the elements of this initiative with industry, consumer groups, and other stakeholders.

The Reclaim Your Name initiative meshes nicely with the FTC's ongoing interest in a universal, simple, persistent, and effective Do Not Track mechanism that allows a consumer to stop companies from mining cyberspace for information about her for marketing purposes. First in 2010,<sup>25</sup> and then again in 2012,<sup>26</sup> the FTC called for a system that would allow consumers to make choices about tracking that would travel with them wherever they went in cyberspace; that would apply across the ecosystem to all types of tracking; that would be easy to find and use; and that would let consumers stop, not just the serving of targeted ads, but the collecting of their personal information as they browsed online or used their mobile devices.

Since 2010, there has been progress toward our vision of Do Not Track. Major browsers permit users to send instructions not to track across websites. The Digital Advertising Alliance has deployed an icon-based opt-out system – the About Ads Program – and has promised to work collaboratively with browsers so that consumers' choices will be persistent and honored no matter how they are initially exercised. And an international standards-setting organization – the W3C – has convened a working group to create a universal Do Not Track standard through a consensus-based process with representatives from across the spectrum of stakeholders. I urge the W3C stakeholders to forge ahead with their work and reach consensus.

If consensus is reached, Do Not Track would allow consumers to choose when their online data is monitored for marketing purposes. Reclaim Your Name would give consumers the power to access online and offline data already collected, exercise some choice over how their data will be used in the commercial sphere, and correct any errors in information being used by those making decisions materially impacting consumers' lives. Together, these policies will restore consumers' rights to privacy that big data has not just challenged but has abrogated in too many instances.

One of our nation's greatest social and political thinkers – the late Abigail Van Buren of “Dear Abby” fame – often said “No one can take advantage of you without your permission.” That is such a perfectly American thought that I am surprised Jefferson didn't include it in his list of the truths we hold to be self-evident. It speaks to American self-reliance and independence – to our individual rights set in stone in the Declaration of Independence and the Bill of Rights.

And perhaps therein lies the biggest challenge of big data: it is taking advantage of us without our permission. Often without consent or warning, and sometimes in

---

<sup>25</sup> Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, A Preliminary FTC Staff Report (Dec. 1, 2010) at 63 – 68, available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

<sup>26</sup> 2012 Privacy Report, *supra* note 10, at 52 – 55.



completely surprising ways, big data analysts are tracking our every click and purchase, examining them to determine exactly who we are – establishing our name, good or otherwise – and retaining the information in dossiers that we know nothing about, much less consent to.

There is no reason that big data cannot coexist with an effective Do Not Track mechanism and with a system that empowers consumers to make real choices about how their private information will be used. The ability to claim your name – or in the case of big data, Reclaim Your Name – is as American as Mom and apple pie. I can't believe consumers will give that up easily, even for all the convenience, entertainment and wonder that cyberspace currently has on offer. And I want to believe that industries currently fueled by big data will join together to help consumers reclaim their names.

## NOTES

## NOTES

Digital Advertising Alliance, Application of  
the Self-Regulatory Principles of  
Transparency and Control to Data Used  
Across Devices (November 2015)

Submitted by:

Noga Rosenthal

*Epsilon/Conversant*

Reprinted with permission.

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



# Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices



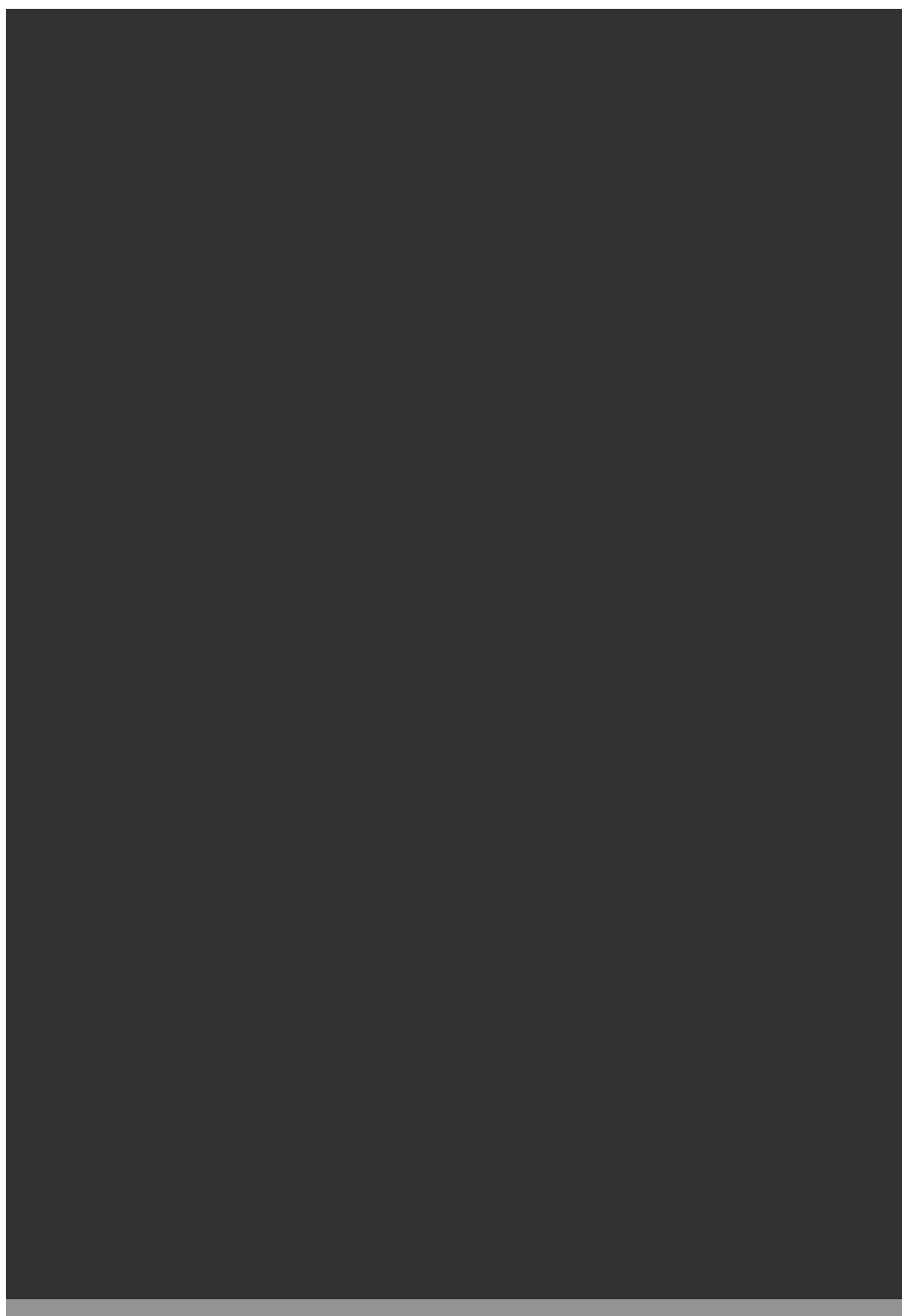
DIGITAL ADVERTISING ALLIANCE  
[www.AboutAds.info](http://www.AboutAds.info)

NOVEMBER 2015



**DEVELOPED BY:** American Association of Advertising Agencies  
American Advertising Federation  
Association of National Advertisers  
Council of Better Business Bureaus  
Direct Marketing Association  
Interactive Advertising Bureau  
Network Advertising Initiative

**COUNSEL:** Venable LLP  
Stuart P. Ingis  
Michael A. Signorelli  
Robert L. Hartwell



# Application of the DAA Principles of Transparency and Control to Data Used Across Devices

## OVERVIEW

This guidance explains how the existing Digital Advertising Alliance (“DAA”) Self-Regulatory Principles for Online Behavioral Advertising (“OBA Principles”) and Multi-Site Data (“MSD Principles”), and the Application of the Self-Regulatory Principles to the Mobile Environment (“Mobile Guidance”) (collectively, the “Principles”) apply to the practice of using Multi-Site Data and Cross-App Data collected from a particular browser or device for use on a different computer or device.

The OBA Principles set forth guidance for when data is collected and used to predict user preferences or interests to deliver advertising to that specific computer or device on which such data was collected.<sup>1</sup>

Subsequent to the adoption of the OBA Principles, the DAA adopted the MSD Principles in November of 2011 to extend the choice provided for OBA beyond advertising to all uses of Multi-Site Data with enumerated purpose limitations. The MSD Principles are built off

---

<sup>1</sup> See definition of Online Behavioral Advertising, *Self-Regulatory Principles for Online Behavioral Advertising* at p. 10(G).



of the OBA Principles and by extension also limit the corresponding choice to consumers that was extended to Multi-Site Data to data used on the specific computer or device on which such data was collected.<sup>2</sup>

As the adoption and use of devices has exploded in recent years, so have the practices and benefits to consumers of integrating and using data collected across devices.<sup>3</sup> This guidance is intended to clarify how the Transparency and Consumer Control principles apply to the use of Multi-Site Data and Cross-App Data across devices. The limitations and restrictions set forth in this document are within the scope of the Digital Advertising Alliance accountability programs.

---

<sup>2</sup> See Multi-Site Principles at p. 1. In 2013, DAA issued guidance on the application of the Principles to the mobile environment, *See Application of Self-Regulatory Principles to the Mobile Environment* (2013) ("Mobile Guidance") available at [http://www.aboutads.info/DAA\\_Mobile\\_Guidance.pdf](http://www.aboutads.info/DAA_Mobile_Guidance.pdf).

<sup>3</sup> As described in the DAA Principles, the relevant Transparency and Consumer Control requirements apply to an entity's collection or use of Multi-Site Data and/or Cross-App Data, whether or not that collection or use occurs on a single device or across multiple devices, and also apply to the extent Multi-Site Data and/or Cross-App Data is combined with data that is outside the scope of the DAA Principles.

## TRANSPARENCY

In providing Transparency as set forth in the existing Principles, entities collecting Multi-Site Data and Cross-App Data from a particular browser or device for use on a different computer or device should include in the notice on their own Web sites that describes their data collection and use practices the fact that data collected from a particular browser or device may be used with another computer or device that is linked to the browser or device on which such data was collected, or transferred to a non-Affiliate for such purposes.<sup>4</sup> Likewise, the Transparency should include a description of the fact that exercising choice through the consumer choice mechanism limits such collection and use as set forth in the Control Section.<sup>5</sup>

When data is collected or used on a Web site or through an application, consistent with the existing principles, the First Party should provide a clear, meaningful, and prominent link to a disclosure that either links to the industry developed Web site(s) or choice mechanism that provides control consistent with this guidance or that individually lists Third Parties engaged in the collection of Multi-Site or Cross-App Data through its Web site or application.<sup>6</sup>

---

<sup>4</sup> Consistent with the OBA Principles, MSD Principles, and Mobile Guidance, this notice should be provided on a Third Party's own Web site(s) or accessible from application(s) from or through which they collect Cross-App Data (*see* OBA Principles at p. 12; Mobile Guidance at p. 14). This notice should also indicate the Third Party's collection and use of Precise Location Data for use across devices. Consent for the collection and use of Precise Location Data should encompass the collection of Precise Location Data from a device for use on another computer or device that is linked to the device where Consent is obtained.

<sup>5</sup> Consistent with the existing DAA Principles, Third Parties should provide Enhanced Notice with respect to this notice as set forth in the OBA Principles and Mobile Guidance (*see* OBA Principles at p. 13; Mobile Guidance at pp. 14-15).

<sup>6</sup> *See* OBA Principles at p. 35. Consistent with the existing DAA Principles, a Website does not need to include such a link in instances where the Third Party provides Transparency as described in OBA Principles II.A.2(a).

## CONTROL

The choice made by consumers as set forth in the existing Principles regarding the collection and use of data for purposes other than those set forth in the sections on Purpose Limitations,<sup>7</sup> also applies to:<sup>8</sup>

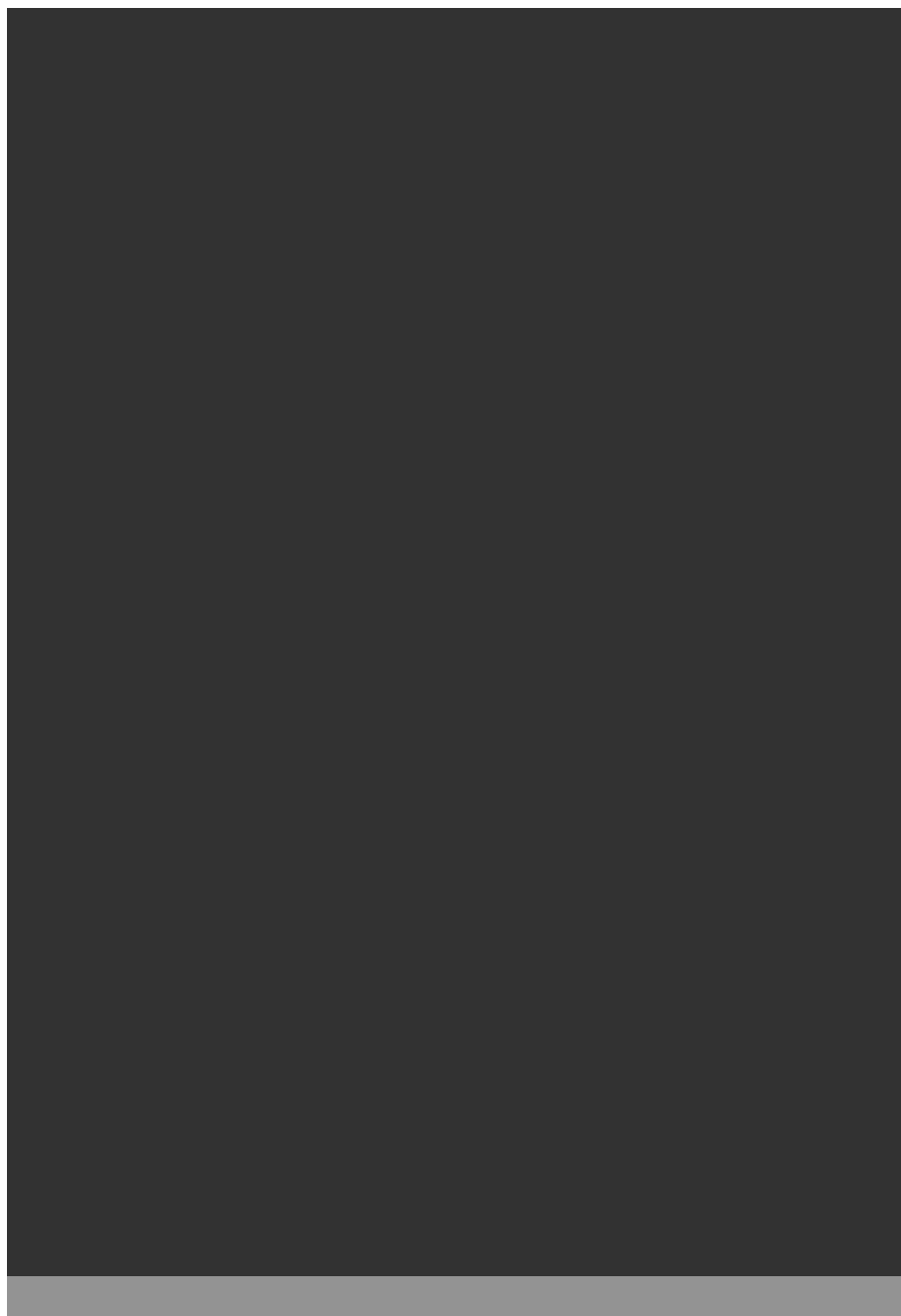
- The collection of Multi-Site Data on the browser, or Cross-App Data on the device, on which choice is being exercised, for use on another computer or device that is linked with the browser or device on which the choice is being exercised;
- The use of Multi-Site Data or Cross-App Data on the browser or device on which choice is being exercised when that data was collected on another computer or device that is linked with the browser or device on which choice is being exercised; and
- The transfer to a Non-Affiliate of Multi-Site Data and/or Cross-App Data collected from the browser or device on which choice is being exercised.<sup>9</sup>

\* \* \*

<sup>7</sup> MSD Principles at pp. 1-2 and Mobile Guidance at pp. 30-31.

<sup>8</sup> This control provision does not address choice with regard to the creation of a “graph.”

<sup>9</sup> Consistent with the DAA Principles, a Third Party that provides consumers access to a mechanism or setting offered by a platform or operating system that provides the ability to exercise choice with respect to Cross-App Data in a manner consistent with this guidance document satisfies this guidance. (See Mobile Guidance at p. 19). An entity cannot avoid the Principles’ Transparency and Consumer Control obligations by transferring data to an Affiliate for use by that Affiliate or by using the data on a different browser or device than the browser or device on which it was collected. Additionally, choice under this guidance document applies to future data collection, use, and transfer for purposes other than those set forth in the sections on Purpose Limitations.





## NOTES

## NOTES

13

U.S. Federal Trade Commission,  
Press Release, FTC Warns Marketers  
That Mobile Apps May Violate Fair Credit  
Reporting Act (February 7, 2012)

Submitted by:  
Noga Rosenthal  
*Epsilon/Conversant*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.







**FEDERAL TRADE COMMISSION**  
PROTECTING AMERICA'S CONSUMERS

# FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act

## Agency Sends Letter to Marketers of Six Apps for Background Screening

FOR RELEASE

February 7, 2012

**TAGS:** [Fair Credit Reporting Act \(FCRA\)](#) | [Consumer Protection](#) | [Credit and Finance](#) | [Credit Reporting](#) | [Privacy and Security](#)

The Federal Trade Commission warned marketers of six mobile applications that provide background screening apps that they may be violating the Fair Credit Reporting Act. The FTC warned the apps marketers that, if they have reason to believe the background reports they provide are being used for employment screening, housing, credit, or other similar purposes, they must comply with the Act.

The companies that received the letters are [Everify, Inc.](#), marketer of the Police Records app, [InfoPay, Inc.](#), marketer of the Criminal Pages app, and [Intelligator, Inc.](#), marketer of Background Checks, Criminal Records Search, Investigate and Locate Anyone, and People Search and Investigator apps.

According to the FTC, some of the apps include criminal record histories, which bear on an individual's character and general reputation and are precisely the type of information that is typically used in employment and tenant screening.

"If you have reason to believe that your background reports are being used for employment or other FCRA purposes, you and your customers who are using your reports for such purposes must comply with the FCRA," the letters say.

The FCRA is designed to protect the privacy of consumer report information and ensure that the information supplied by consumer reporting agencies is accurate. Consumer reports are communications that include information on an individual's character, reputation, or personal characteristics and are used or expected to be used for purposes such as employment, housing or credit.

Under the FCRA, operations that assemble or evaluate information to provide to third parties qualify as consumer reporting agencies, or CRAs. Mobile apps that supply such information may qualify as CRAs under the Act. CRAs must take reasonable steps to ensure the user of each report has a 'permissible purpose' to use the report; take reasonable steps to ensure the maximum possible accuracy of the information conveyed in its reports; and provide users of its reports with information about their obligations under the FCRA. In the case of consumer reports provided for employment purposes, for example, CRAs must provide employers with information regarding their obligation to provide notice to employees and applicants of any adverse action taken on the basis of a consumer report.

According to the letters, the agency has made no determination whether the companies are violating the FCRA, but encourages them to review their apps and their policies and procedures to be sure they comply with the FCRA.

The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC's online [Complaint Assistant](#) or call 1-877-FTC-HELP (1-877-382-4357). The FTC enters complaints into Consumer Sentinel, a secure, online database available to more than 2,000 civil and criminal law enforcement agencies in the U.S. and abroad. Like the FTC on [Facebook](#), follow us on [Twitter](#), and [subscribe to press releases](#) for the latest FTC news and resources.

## Contact Information

### MEDIA CONTACT:

Claudia Bourne Farrell  
*Office of Public Affairs*  
202-326-2181

### STAFF CONTACT:

Anthony Rodríguez  
*Bureau of Consumer Protection*  
202-326-2757



ftc.gov

## NOTES

## NOTES

14

U.S. Federal Trade Commission, Big Data:  
A Tool for Inclusion or Exclusion?  
Understanding the Issues (January 2016)

Submitted by:  
Noga Rosenthal  
*Epsilon/Conversant*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



# BIG DATA

A Tool for  
Inclusion or Exclusion?

---

UNDERSTANDING THE ISSUES

FTC REPORT

FEDERAL TRADE COMMISSION  
JANUARY 2016





# Big Data

## A Tool for Inclusion or Exclusion?

---

### UNDERSTANDING THE ISSUES

#### FTC REPORT

JANUARY 2016



#### FEDERAL TRADE COMMISSION

Edith Ramirez, Chairwoman

Julie Brill, Commissioner

Maureen K. Ohlhausen, Commissioner

Terrell McSweeney, Commissioner



# Contents

<b>Executive Summary .....</b>	<b>i</b>
<b>I. Introduction .....</b>	<b>1</b>
<b>II. Life Cycle of Big Data .....</b>	<b>3</b>
<b>III. Big Data's Benefits and Risks .....</b>	<b>5</b>
<b>IV. Considerations for Companies in Using Big Data .....</b>	<b>12</b>
A. Potentially Applicable Laws .....	12
Questions for Legal Compliance .....	24
B. Special Policy Considerations Raised by Big Data Research .....	25
Summary of Research Considerations .....	32
<b>V. Conclusion .....</b>	<b>33</b>
<b>Appendix:</b>	
<b>Separate Statement of Commissioner Maureen K. Ohlhausen .....</b>	<b>A-1</b>



## Executive Summary

We are in the era of big data. With a smartphone now in nearly every pocket, a computer in nearly every household, and an ever-increasing number of Internet-connected devices in the marketplace, the amount of consumer data flowing throughout the economy continues to increase rapidly.

The analysis of this data is often valuable to companies and to consumers, as it can guide the development of new products and services, predict the preferences of individuals, help tailor services and opportunities, and guide individualized marketing. At the same time, advocates, academics, and others have raised concerns about whether certain uses of big data analytics may harm consumers, particularly low-income and underserved populations.

To explore these issues, the Federal Trade Commission (“FTC” or “the Commission”) held a public workshop, *Big Data: A Tool for Inclusion or Exclusion?*, on September 15, 2014. The workshop brought together stakeholders to discuss both the potential of big data to create opportunities for consumers and to exclude them from such opportunities. The Commission has synthesized the information from the workshop, a prior FTC seminar on alternative scoring products, and recent research to create this report. Though “big data” encompasses a wide range of analytics, this report addresses only the commercial use of big data consisting of consumer information and focuses on the impact of big data on low-income and underserved populations. Of course, big data also raises a host of other important policy issues, such as notice, choice, and security, among others. Those, however, are not the primary focus of this report.

As “little” data becomes “big” data, it goes through several phases. The life cycle of big data can be divided into four phases: (1) collection; (2) compilation and consolidation; (3) analysis; and (4) use. This report focuses on the fourth phase and discusses the benefits and risks created by the use of big data analytics; the consumer protection and equal opportunity laws that currently apply to big data; research in the field of big data; and lessons that companies should take from the research. Ultimately, this report is intended to educate businesses on important laws and research that are relevant to big data analytics and provide suggestions aimed at maximizing the benefits and minimizing its risks.

### Big Data’s Benefits and Risks

Big data analytics can provide numerous opportunities for improvements in society. In addition to more effectively matching products and services to consumers, big data can create opportunities for low-income and underserved communities. For example, workshop participants and others have noted that big data is helping target educational, credit, healthcare, and employment opportunities to low-income and underserved populations. At the same time, workshop participants and others have noted how potential inaccuracies and biases might lead to detrimental effects for low-income and underserved populations. For example, participants raised concerns that companies could use big data to exclude low-income and underserved communities from credit and employment opportunities.

## Consumer Protection Laws Applicable to Big Data

Workshop participants and commenters discussed how companies can use big data in ways that provide benefits to themselves and society, while minimizing legal and ethical risks. Specifically, they noted that companies should have an understanding of the various laws, including the Fair Credit Reporting Act, equal opportunity laws, and the Federal Trade Commission Act, that may apply to big data practices.

### 1. Fair Credit Reporting Act

The Fair Credit Reporting Act (“FCRA”) applies to companies, known as consumer reporting agencies or CRAs, that compile and sell consumer reports, which contain consumer information that is used or expected to be used for credit, employment, insurance, housing, or other similar decisions about consumers’ eligibility for certain benefits and transactions. Among other things, CRAs must implement reasonable procedures to ensure maximum possible accuracy of consumer reports and provide consumers with access to their own information, along with the ability to correct any errors.

Traditionally, CRAs include credit bureaus, employment background screening companies, and other specialty companies that provide particularized services for making consumer eligibility decisions, such as check authorizations or tenant screenings. Some data brokers may also be considered CRAs subject to the FCRA, particularly if they advertise their services for eligibility purposes. The Commission has entered into a number of consent decrees with data brokers that advertise their consumer profiles for employment and tenant screening purposes. Companies that use consumer reports also have obligations under the FCRA.

Workshop panelists and commenters discussed a growing trend in big data, in which companies may be purchasing predictive analytics products for eligibility determinations. Under traditional credit scoring models, companies compare known credit characteristics of a consumer—such as past late payments—with historical data that shows how people with the same credit characteristics performed over time in meeting their credit obligations. Similarly, predictive analytics products may compare a known characteristic of a consumer to other consumers with the same characteristic to predict whether that consumer will meet his or her credit obligations. The difference is that, rather than comparing a traditional credit characteristic, such as debt payment history, these products may use non-traditional characteristics—such as a consumer’s zip code, social media usage, or shopping history—to create a report about the creditworthiness of consumers that share those non-traditional characteristics, which a company can then use to make decisions about whether that consumer is a good credit risk. The standards applied to determine the applicability of the FCRA in a Commission enforcement action, however, are the same.

Only a fact-specific analysis will ultimately determine whether a practice is subject to or violates the FCRA, and as such, companies should be mindful of the law when using big data analytics to make FCRA-covered eligibility determinations.

## 2. Equal Opportunity Laws

Companies should also consider a number of federal equal opportunity laws, including the Equal Credit Opportunity Act (“ECOA”), Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Housing Act, and the Genetic Information Nondiscrimination Act. These laws prohibit discrimination based on protected characteristics such as race, color, sex or gender, religion, age, disability status, national origin, marital status, and genetic information.

Of these laws, the FTC enforces ECOA, which prohibits credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or because a person receives public assistance. To prove a violation of ECOA, plaintiffs typically must show “disparate treatment” or “disparate impact.” Disparate treatment occurs when a creditor treats an applicant differently based on a protected characteristic. For example, a lender cannot refuse to lend to single persons or offer less favorable terms to them than married persons even if big data analytics show that single persons are less likely to repay loans than married persons. Disparate impact occurs when a company employs facially neutral policies or practices that have a disproportionate adverse effect or impact on a protected class, unless those practices or policies further a legitimate business need that cannot reasonably be achieved by means that are less disparate in their impact. For example, if a company makes credit decisions based on consumers’ zip codes, such decisions may have a disparate impact on particular ethnic groups because certain ethnic groups are concentrated in particular zip codes. Accordingly, the practice may be a violation of ECOA. The analysis turns on whether the decisions have a disparate impact on a protected class and are not justified by a legitimate business necessity. Even if evidence shows the decisions are justified by a business necessity, if there is a less discriminatory alternative, the decisions may still violate ECOA.

Workshop discussions focused on whether advertising could implicate equal opportunity laws. In most cases, a company’s advertisement to a particular community for a credit offer that is open to all to apply is unlikely, by itself, to violate ECOA, absent disparate treatment or an unjustified disparate impact in subsequent lending. Nevertheless, companies should proceed with caution in this area. For advertisements relating to credit products, companies should look to Regulation B, which is the implementing regulation for ECOA. It prohibits creditors from making oral or written statements, in advertising or otherwise, to applicants or prospective applicants that would discourage on a prohibited basis a reasonable person from making or pursuing an application. With respect to prescreened solicitations, Regulation B also requires creditors to maintain records of the solicitations and the criteria used to select potential recipients. Advertising and marketing practices could impact a creditor’s subsequent lending patterns and the terms and conditions of the credit received by borrowers, even if credit offers are open to all who apply. In some cases, the Department of Justice has cited a creditor’s advertising choices as evidence of discrimination.



Ultimately, as with the FCRA, whether a practice is unlawful under equal opportunity laws is a case-specific inquiry, and as such, companies should proceed with caution when their practices could result in disparate treatment or have a demonstrable disparate impact based on protected characteristics.

### 3. The Federal Trade Commission Act

Workshop participants and commenters also discussed the applicability of Section 5 of the Federal Trade Commission Act (“FTC Act”), which prohibits unfair or deceptive acts or practices, to big data analytics. Companies engaging in big data analytics should consider whether they are violating any material promises to consumers—whether that promise is to refrain from sharing data with third parties, to provide consumers with choices about sharing, or to safeguard consumers’ personal information—or whether they have failed to disclose material information to consumers. In addition, companies that maintain big data on consumers should take care to reasonably secure consumers’ data. Further, at a minimum, companies must not sell their big data analytics products to customers if they know or have reason to know that those customers will use the products for fraudulent or discriminatory purposes. The inquiry will be fact-specific, and in every case, the test will be whether the company is offering or using big data analytics in a deceptive or unfair way.

### Research on Big Data

Workshop participants, academics, and others also addressed the ways big data analytics could affect low-income, underserved populations, and protected groups. Some pointed to research that demonstrates that there is a potential for incorporating errors and biases at every stage—from choosing the data set used to make predictions, to defining the problem to be addressed through big data, to making decisions based on the results of big data analysis—which could lead to potential discriminatory harms. Others noted that these concerns are overstated or simply not new, and emphasized that rather than disadvantaging minorities, big data can create opportunities for low-income and underserved populations.

To maximize the benefits and limit the harms of big data, the Commission encourages companies to consider the following questions raised by research in this area:

- **How representative is your data set?** Companies should consider whether their data sets are missing information about certain populations, and take steps to address issues of underrepresentation and overrepresentation. For example, if a company targets services to consumers who communicate through an application or social media, they may be neglecting populations that are not as tech-savvy.
- **Does your data model account for biases?** Companies should consider whether biases are being incorporated at both the collection and analytics stages of big data’s life cycle, and develop strategies to overcome them. For example, if a company has a big data algorithm that only considers applicants from “top tier” colleges to help them make hiring decisions, they may be incorporating previous biases in college admission decisions.

- **How accurate are your predictions based on big data?** Companies should remember that while big data is very good at detecting correlations, it does not explain which correlations are meaningful. A prime example that demonstrates the limitations of big data analytics is Google Flu Trends, a machine-learning algorithm for predicting the number of flu cases based on Google search terms. While, at first, the algorithms appeared to create accurate predictions of where the flu was more prevalent, it generated highly inaccurate estimates over time. This could be because the algorithm failed to take into account certain variables. For example, the algorithm may not have taken into account that people would be more likely to search for flu-related terms if the local news ran a story on a flu outbreak, even if the outbreak occurred halfway around the world.
- **Does your reliance on big data raise ethical or fairness concerns?** Companies should assess the factors that go into an analytics model and balance the predictive value of the model with fairness considerations. For example, one company determined that employees who live closer to their jobs stay at these jobs longer than those who live farther away. However, another company decided to exclude this factor from its hiring algorithm because of concerns about racial discrimination, particularly since different neighborhoods can have different racial compositions.

The Commission encourages companies to apply big data analytics in ways that provide benefits and opportunities to consumers, while avoiding pitfalls that may violate consumer protection or equal opportunity laws, or detract from core values of inclusion and fairness. For its part, the Commission will continue to monitor areas where big data practices could violate existing laws, including the FTC Act, the FCRA, and ECOA, and will bring enforcement actions where appropriate. The Commission will also continue to examine and raise awareness about big data practices that could have a detrimental impact on low-income and underserved populations, and promote the use of big data that has a positive impact on such populations.



## I. Introduction

The era of big data has arrived. While companies historically have collected and used information about their customer interactions to help improve their operations, the expanding use of online technologies has greatly increased the amount of consumer data that flows throughout the economy. In many cases, when consumers engage digitally—whether by shopping, visiting websites, paying bills, connecting with family and friends through social media, using mobile applications, or using connected devices, such as fitness trackers or smart televisions—companies collect information about their choices, experiences, and individual characteristics. The analysis of this consumer information is often valuable to companies and to consumers, as it provides insights into market-wide tastes and emerging trends, which can guide the development of new products and services. It is also valuable to predict the preferences of specific individuals, help tailor services, and guide individualized marketing of products and services.

The term “big data” refers to a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions.<sup>1</sup>

A common framework for characterizing big data relies on the “three Vs,” the volume, velocity, and variety of data, each of which is growing at a rapid rate as technological advances permit the analysis and use of this data in ways that were not possible previously.<sup>2</sup> Volume refers to the vast quantity of data that can be gathered and analyzed effectively. The costs of collecting and storing data continue to drop dramatically. And the ability to access millions of data points increases the predictive power of consumer data analysis.

- 1 See, e.g., EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 2–3 (2014) [hereinafter “WHITE HOUSE MAY 2014 REPORT”], [http://www.whitehouse.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_5.1.14\\_final\\_print.pdf](http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf); Jim Thatcher, *Living on Fumes: Digital Footprints, Data Fumes, and the Limitations of Spatial Big Data*, 8 INT’L J. OF COMM’N 1765, 1767–69 (2014), <http://ijoc.org/index.php/ijoc/article/view/2174/1158>. See also Comment #00018 from Persis Yu, Nat’l Consumer L. Ctr., to Fed. Trade Comm’n, attached report at 10 (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00018-92374.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00018-92374.pdf).
- 2 See, e.g., Transcript of Big Data: A Tool for Inclusion or Exclusion?, in Washington, D.C. (Sept. 15, 2014), at 15 (Solon Barocas), 32 (Joseph Turow), 40–41 (Joseph Turow), 261 (Christopher Wolf) [hereinafter Big Data Tr.], [https://www.ftc.gov/system/files/documents/public\\_events/313371/bigdata-transcript-9\\_15\\_14.pdf](https://www.ftc.gov/system/files/documents/public_events/313371/bigdata-transcript-9_15_14.pdf). See also WHITE HOUSE MAY 2014 REPORT, *supra* note 1, at 4–5; Comment #00067 from Mark MacCarthy, Software & Info. Indus. Assoc., to Fed. Trade Comm’n 2 (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00067-92918.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00067-92918.pdf); Comment #00065 from Jules Polonetsky & Christopher Wolf, Future of Privacy Forum, to Fed. Trade Comm’n 2 (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00065-92921.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00065-92921.pdf); Comment #00049 from Martin Abrams, Info. Accountability Found., to Fed. Trade Comm’n 3–4 & n.6, [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00049-92780.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00049-92780.pdf); Comment #00031 from M. Gary LaFever & Ted Myerson, anonos, to Fed. Trade Comm’n 1 (Aug. 21, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00031-92442.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00031-92442.pdf). Others suggest that there is a “fourth V,” veracity, to denote the accuracy and integrity of data used. See, e.g., Brian Gentile, *The New Factors of Production and the Rise of Data-Driven Applications*, FORBES (Oct. 31, 2011), <http://www.forbes.com/sites/ciocentral/2011/10/31/the-new-factors-of-production-and-the-rise-of-data-driven-applications/>.

Velocity is the speed with which companies can accumulate, analyze, and use new data. Technological improvements allow companies to harness the predictive power of data more quickly than ever before, sometimes instantaneously.<sup>3</sup>

Variety means the breadth of data that companies can analyze effectively. Companies can now combine very different, once unlinked, kinds of data—either on their own or through data brokers or analytics firms—to infer consumer preferences and predict consumer behavior, for example.

Together, the three Vs allow for more robust research and correlation. Previously, finding a representative data sample sufficient to produce statistically significant results could be very difficult and expensive. Today, the present scope and scale of data collection enables cost-effective, substantial research of even obscure or mundane topics (e.g., the amount of foot traffic in a park at different times of day).

Big data can produce tremendous benefits for society, such as advances in medicine, education, health, and transportation, and in many instances, without using consumers' personally identifiable information. Big data also can allow companies to improve their offerings, provide consumers with personalized goods and services, and match consumers with products they are likely to be interested in. At the same time, advocates, academics, and others have raised concerns about whether certain uses of big data analytics may harm consumers. For example, if big data analytics incorrectly predicts that particular consumers are not likely to respond to prime credit offers, certain types of educational opportunities, or job openings requiring a college degree, companies may miss a chance to reach individuals that desire this information. In addition, if big data analytics incorrectly predicts that particular consumers are not good candidates for prime credit offers, educational opportunities, or certain lucrative jobs, such educational opportunities, employment, and credit may never be offered to these consumers. Some fear that such incorrect predictions could perpetuate existing disparities.

To examine these issues, the Federal Trade Commission ("FTC" or "the Commission") held a public workshop, *Big Data: A Tool for Inclusion or Exclusion?*, on September 15, 2014.<sup>4</sup> In particular, the workshop explored the potential impact of big data on low-income and underserved populations. The workshop brought together academics, government representatives, consumer advocates, industry representatives, legal practitioners, and others to discuss the potential of big data to create opportunities for consumers or exclude them from such opportunities. The workshop consisted of four panels addressing the following topics: (1) current uses of big data; (2) potential uses of big data; (3) the application of equal opportunity and consumer protection laws to big data; and (4) best practices to enhance consumer protection in the use of big data. The Commission also received sixty-five public comments on these issues from private citizens, industry representatives, trade groups, consumer and privacy advocates, think tanks, and academics.

<sup>3</sup> WHITE HOUSE MAY 2014 REPORT, *supra* note 1, at 5.

<sup>4</sup> The materials from the workshop are available on the FTC website at <http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion>.

The Commission has synthesized the discussions and comments from the workshop—along with the record from a prior FTC seminar on alternative scoring products<sup>5</sup> and recent research—to create this report, which focuses on the impact of big data on low-income and underserved populations. The report is divided into four sections. First, the report describes the “life cycle” of big data and how “little” data turns into big data. Second, it discusses some of the benefits and risks created by the use of big data. Third, it describes some of the consumer protection laws that currently apply to big data. Finally, it discusses certain research in the field of big data and lessons that companies should take from the research in order to help them maximize the benefits of big data while mitigating risks. Importantly, though the term “big data” encompasses a wide range of analytics, this report addresses only the commercial use of big data consisting of consumer information.<sup>6</sup>

## II. Life Cycle of Big Data

The life cycle of big data can be divided into four phases: (1) collection; (2) compilation and consolidation; (3) data mining and analytics; and (4) use.<sup>7</sup>

As to the first step, not all data starts as big data. Rather, companies collect bits of data from a variety of sources.<sup>8</sup> For example, as consumers browse the web or shop online, companies can track and link their activities. Sometimes consumers log into services or identify themselves when they make a purchase. Other

5 On March 19, 2014, the Commission hosted a seminar on alternative scoring products and received nine public comments in connection with the seminar. *Spring Privacy Series: Alternative Scoring Products*, FED. TRADE COMM’N (Mar. 19, 2014), <http://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products>.

6 The report does include some examples from non-commercial fields, but it is intended to guide companies as they use big data about consumers.

7 See, e.g., Nat’l Consumer L. Ctr. Comment #00018, *supra* note 1, attached report at 11–12. In May 2014, the Commission released a report studying data brokers, which focused on the first three phases of the life cycle of big data. FED. TRADE COMM’N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014) [hereinafter “DATA BROKERS REPORT”], <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

8 See generally Comment #00055 from Daniel Castro, Ctr. for Data Innovation, to Fed. Trade Comm’n (Oct. 23, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00055-92856.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00055-92856.pdf); Comment #00026 from Daniel Castro, Ctr. for Data Innovation, to Fed. Trade Comm’n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00026-92395.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00026-92395.pdf); Comment #00024 from Alvaro Bedoya, Ctr. on Privacy & Tech. at Geo. L., to Fed. Trade Comm’n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00024-92434.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00024-92434.pdf); Nat’l Consumer L. Ctr. Comment #00018, *supra* note 1; Comment #00016 from James Steyer, Common Sense Media, to Fed. Trade Comm’n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00016-92371.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00016-92371.pdf); Comment #00015 from Nathan Newman, N.Y.U. Info. L. Inst., to Fed. Trade Comm’n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00015-92370.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf); Comment #00010 from Thomas Lenard, Tech. Pol’y Inst., to Fed. Trade Comm’n (July 28, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/07/00010-92280.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/07/00010-92280.pdf); Comment #00003 from Jeff Chester, Ctr. for Dig. Democracy, & Edmund Mierzwinski, U.S. PIRG Educ. Fund, to Fed. Trade Comm’n (May 9, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/05/00003-90097.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/05/00003-90097.pdf).

times, techniques such as tracking cookies,<sup>9</sup> browser or device fingerprinting,<sup>10</sup> and even history sniffing<sup>11</sup> identify who consumers are, what they do, and where they go. In the mobile environment, companies track and link consumers' activities across applications as another method of gathering information about their habits and preferences. More broadly, cross-device tracking offers the ability to interact with the same consumer across her desktop, laptop, tablet, wearable, and smartphone, using both online and offline information.<sup>12</sup> Companies also are gathering data about consumers across the Internet of Things—the millions of Internet-connected devices that are in the market.<sup>13</sup> Finally, data collection occurs offline as well, for example, through loyalty programs, warranty cards, surveys, sweepstakes entries, and even credit card purchases.<sup>14</sup>

After collection, the next step in the life cycle of big data is compilation and consolidation. Commercial entities that compile data include online ad networks, social media companies, and large banks or retailers.<sup>15</sup> One important category of commercial entities that compile and consolidate data is data brokers. They combine data from disparate sources to build profiles about individual consumers. Indeed, some data brokers store billions of data elements on nearly every U.S. consumer.<sup>16</sup>

The third step is data analytics. One form of analytics is descriptive—the objective is to uncover and summarize patterns or features that exist in data sets.<sup>17</sup> By contrast, predictive data analytics refers to the use

9 Tracking cookies are a specific type of cookie that is distributed, shared, and read across two or more unrelated websites for the purpose of gathering information or presenting customized data to a consumer. See *Tracking Cookie*, SYMANTEC, [https://www.symantec.com/security\\_response/writeup.jsp?docid=2006-080217-3524-99](https://www.symantec.com/security_response/writeup.jsp?docid=2006-080217-3524-99) (last visited Dec. 29, 2015).

10 “Browser fingerprinting” is a method of tracking web browsers by the configuration and settings information they make visible to websites, rather than traditional tracking methods” such as cookies. *Panopticklick: Is Your Browser Safe Against Tracking?*, ELEC. FRONTIER FOUND., <https://panopticklick.eff.org/about#browser-fingerprinting> (last visited Dec. 29, 2015).

11 History sniffing is the practice of tracking which sites a user has or has not visited. See Ben Schott, *History Sniffing*, N.Y. TIMES (Dec. 8, 2010), [http://schott.blogs.nytimes.com/2010/12/08/history-sniffing/?\\_r=0](http://schott.blogs.nytimes.com/2010/12/08/history-sniffing/?_r=0). See also Brian Krebs, *What You Should Know About History Sniffing*, KREBS ON SEC. (Dec. 6, 2010), <http://krebsonsecurity.com/2010/12/what-you-should-know-about-history-sniffing/>.

12 In November 2015, the Commission held a workshop to study the various alternative techniques used to track consumers across their devices. See *Cross-Device Tracking*, FED. TRADE COMM’N (Nov. 16, 2015), <https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking>.

13 In January 2015, the Commission released a staff report entitled, *INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD*, recommending steps businesses can take to enhance and protect consumers’ privacy and security as it relates to Internet-connected devices. FED. TRADE COMM’N, *INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD* (2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

14 See, e.g., DATA BROKERS REPORT, *supra* note 7, at 11–15.

15 See generally Nat’l Consumer L. Ctr. Comment #00018, *supra* note 1; N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8.

16 See, e.g., DATA BROKERS REPORT, *supra* note 7, at 46–47.

17 See, e.g., Big Data Tr. 17 (Solon Barocas) (“[W]e can define data mining as the automated process of extracting useful patterns from large data sets, and in particular, patterns that can serve as a basis for subsequent decision making.”). See also JURE LESKOVEC ET AL., *MINING OF MASSIVE DATA SETS* 1, 1 (2014), <http://www.mmds.org/> (characterizing “data mining” as “the construction of a *statistical model*, that is, an underlying distribution from which the visible data is drawn”) (emphasis in original).

of statistical models to generate new data.<sup>18</sup> Developing and testing the models that find patterns and make predictions can require the collection and use of copious amounts of data.<sup>19</sup> In a market context, a common purpose of big data analytics is to draw inferences about consumers' likely choices. Companies may decide to adopt big data analytics to better understand consumers, potentially by using data to attribute to an individual the qualities of those who appear statistically similar, e.g., those who have made similar decisions in similar situations in the past. Thus, a retail firm might use data on its customers' past purchases, web searches, shopping habits, and prices paid to create a statistical model of consumers' purchases at different prices. With that model, the retailer could then compare a prospective consumer's characteristics or past purchases, web searches, and location information to predict how likely the consumer is to purchase a product at various price points.

The final step in the life cycle of big data is use. The Commission's May 2014 report entitled *Data Brokers: A Call for Transparency and Accountability* focused on the first three steps in the life cycle of big data within that industry—collection, compilation, and analytics.<sup>20</sup> It discussed how information gathered for one purpose (e.g., paying for goods and services) could be compiled and analyzed for other purposes, such as for marketing or risk mitigation. In contrast, this report focuses on certain *uses* of big data. It examines the question of how companies use big data to help consumers and the steps they can take to avoid inadvertently harming consumers through big data analytics.

### III. Big Data's Benefits and Risks

Companies have been analyzing data from their own customer interactions on a smaller scale for many years, but the era of big data is still in its infancy.<sup>21</sup> As a result, mining large data sets to find useful, non-obvious patterns is a relatively new but growing practice in marketing, fraud prevention, human resources, and a variety of other fields. Companies are still learning how to deal with big data and unlock its potential while avoiding unintended or unforeseen consequences.<sup>22</sup>

Appropriately employing big data algorithms on data of sufficient quality can provide numerous opportunities for improvements in society. In addition to the market-wide benefits of more efficiently matching products and services to consumers, big data can create opportunities for low-income and

18 See, e.g., Galit Shmueli, *To Explain or Predict?*, 25 STATISTICAL SCI. 289, 291 (2010), <http://www.stat.berkeley.edu/~aldous/157/Papers/shmueli.pdf>. See also Mike Wu, *Big Data Reduction 2: Understanding Predictive Analytics*, SCI. OF SOCIAL BLOG (Mar. 26, 2013 9:41 AM), <http://community.lithium.com/t5/Science-of-Social-blog/Big-Data-Reduction-2-Understanding-Predictive-Analytics/ba-p/79616> ("[P]redictive analytics is all about using *data you have* to predict *data that you don't have*." (emphases in original)).

19 Cf. Comment #00014 from Pam Dixon & Robert Gellman, World Privacy Forum, to Fed. Trade Comm'n 8 (Aug. 14, 2014), <https://www.ftc.gov/policy/public-comments/2014/08/14/comment-00014>.

20 See generally DATA BROKERS REPORT, *supra* note 7.

21 See, e.g., Big Data Tr. 31–32 (Gene Gsell), 32–33 (Joseph Turow), 34 (Mallory Duncan), 107–08 (Pamela Dixon).

22 See, e.g., Big Data Tr. 31–32 (Gene Gsell), 32–33 (Joseph Turow), 78 (danah boyd), 233 (Michael Spadea).



underserved communities.<sup>23</sup> Workshop participants and others have noted that big data is already being used to:

- **Increase educational attainment for individual students.** Educational institutions have used big data techniques to identify students for advanced classes who would otherwise not have been eligible for such classes based on teacher recommendations alone.<sup>24</sup> These institutions have also used big data techniques to help identify students who are at risk of dropping out and in need of early intervention strategies.<sup>25</sup> Similarly, organizations have used big data analytics to demonstrate how certain disciplinary practices, such as school suspensions, affect African-American students far more than Caucasian students, thereby partly explaining the large discrepancy between the graduation rates of these two groups.<sup>26</sup>
- **Provide access to credit using non-traditional methods.** Companies have used big data to provide alternative ways to score populations that were previously deemed unscorable.<sup>27</sup> For example, LexisNexis has created an alternative credit score called RiskView.<sup>28</sup> This product relies on traditional public record information, such as foreclosures and bankruptcies, but it also includes educational history, professional licensure data, and personal property ownership data. Thus, consumers who may not have access to traditional credit, but, for instance, have a professional license, pay rent on time, or own a car, may be given better access to credit than they otherwise would have.<sup>29</sup>

23 See, e.g., Big Data Tr. 83–85 (Mark MacCarthy), 250–51 (Christopher Wolf). See generally Comment #00076 from William Kovacs, U.S. Chamber of Commerce, to Fed. Trade Comm’n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00076-92936.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00076-92936.pdf); Comment #00073 from Michael Beckerman, The Internet Assoc., to Fed. Trade Comm’n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00073-92923.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00073-92923.pdf); Comment #00066 from Carl Szabo, NetChoice, to Fed. Trade Comm’n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00066-92920.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00066-92920.pdf); Comment #00063 from Peggy Hudson, Direct Mktg. Assoc., to Fed. Trade Comm’n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00063-92909.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00063-92909.pdf); Ctr. for Data Innovation Comment #00055, *supra* note 8; Comment #00027 from Jules Polonetsky, Future of Privacy Forum, to Fed. Trade Comm’n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00027-92420.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00027-92420.pdf); Ctr. for Data Innovation Comment #00026, *supra* note 8; Comment #00017 from Mike Zaneis, Interactive Advert. Bureau, to Fed. Trade Comm’n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00017-92372.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00017-92372.pdf); Tech. Pol’y Inst. Comment #00010, *supra* note 8.

24 See, e.g., Big Data Tr. 47–48 (Gene Gsell). Cf. Ctr. for Data Innovation Comment #00055, *supra* note 8, attached report entitled, *THE RISE OF DATA POVERTY IN AMERICA*, at 4–6.

25 See, e.g., Big Data Tr. 84–85 (Mark MacCarthy). See also Software & Info. Indus. Assoc. Comment #00067, *supra* note 2, at 6–7; Ctr. for Data Innovation Comment #00026, *supra* note 8, at 2.

26 See, e.g., Big Data Tr. 250 (Christopher Wolf). See also Future of Privacy Forum Comment #00027, *supra* note 23, attached report entitled, *BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS*, at 9.

27 See, e.g., Big Data Tr. 49–51 (Gene Gsell), 83–84 (Mark MacCarthy), 102–06 (Stuart Pratt), 231–32 (Michael Spadea). See also Software & Info. Indus. Assoc. Comment #00067, *supra* note 2, at 5–6; Tech. Pol’y Inst. Comment #00010, *supra* note 8, at 5–6 & attached report entitled, *BIG DATA, PRIVACY AND THE FAMILIAR SOLUTIONS*, at 7.

28 See, e.g., Software & Info. Indus. Assoc. Comment #00067, *supra* note 2, at 5–6.

29 See, e.g., *Rent Reporting for Credit Building Consulting*, CREDIT BUILDERS ALL., <http://creditbuildersalliance.org/rent-reporting-credit-building-consulting> (last visited Dec. 22, 2015).

Furthermore, big data algorithms could help reveal underlying disparities in traditional credit markets and help companies serve creditworthy consumers from any background.<sup>30</sup>

- **Provide healthcare tailored to individual patients' characteristics.** Organizations have used big data to predict life expectancy, genetic predisposition to disease, likelihood of hospital readmission, and likelihood of adherence to a treatment plan in order to tailor medical treatment to an individual's characteristics.<sup>31</sup> This, in turn, has helped healthcare providers avoid one-size-fits-all treatments and lower overall healthcare costs by reducing readmissions.<sup>32</sup> Ultimately, data sets with richer and more complete data should allow medical practitioners more effectively to perform "precision medicine," an approach for disease treatment and prevention that considers individual variability in genes, environment, and lifestyle.<sup>33</sup>
- **Provide specialized healthcare to underserved communities.** IBM, for example, has worked with hospitals to develop an Oncology Diagnosis and Treatment Advisor. This system synthesizes vast amounts of data from textbooks, guidelines, journal articles, and clinical trials to help physicians make diagnoses and identify treatment options for cancer patients. In rural and low-income areas, where there is a shortage of specialty providers, IBM's Oncology Diagnosis and Treatment Advisor can provide underserved communities with better access to cancer care and lower costs.<sup>34</sup>
- **Increase equal access to employment.** Companies have used big data to help promote a more diverse workforce.<sup>35</sup> Google, for example, recognized that its traditional hiring process was resulting in a homogenous work force. Through analytics, Google identified issues with its hiring process, which included an emphasis on academic grade point averages and "brainteaser" questions

30 See, e.g., Ctr. for Data Innovation Comment #00055, *supra* note 8, attached report entitled, THE RISE OF DATA POVERTY IN AMERICA, at 9. See generally Fair Isaac Corp., *Can Alternative Data Expand Credit Access*, INSIGHTS WHITE PAPER NO. 90 (2015), <http://www.fico.com/en/latest-thinking/white-papers/can-alternative-data-expand-credit-access> (finding that alternative scoring can help lenders safely and responsibly extend credit to many of the more than fifty million U.S. adults who do not currently have FICO scores).

31 See, e.g., Ctr. for Data Innovation Comment #00026, *supra* note 8, at 2. See also Shannon Pettypiece & Jordan Robertson, *Hospitals are Mining Patients' Credit Card Data to Predict Who Will Get Sick*, BLOOMBERG (July 3, 2014), <http://www.bloomberg.com/bw/articles/2014-07-03/hospitals-are-mining-patients-credit-card-data-to-predict-who-will-get-sick>.

32 See, e.g., Ctr. for Data Innovation Comment #00055, *supra* note 8, attached report entitled, THE RISE OF DATA POVERTY IN AMERICA, at 6–8; Future of Privacy Forum Comment #00027, *supra* note 23, attached report entitled, BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS, at 4; Ctr. for Data Innovation Comment #00026, *supra* note 8, at 2. Cf. Software & Info. Indus. Assoc. Comment #00067, *supra* note 2, at 4–5.

33 See, e.g., David Shaywitz, *New Diabetes Study Shows How Big Data Might Drive Precision Medicine*, FORBES (Oct. 30, 2015), <http://www.forbes.com/sites/davidshaywitz/2015/10/30/new-diabetes-study-shows-how-big-data-might-drive-precision-medicine/>.

34 See, e.g., Big Data Tr. 84 (Mark MacCarthy). See also Software & Info. Indus. Assoc. Comment #00067, *supra* note 2, at 4.

35 See, e.g., Big Data Tr. 126 (Mark MacCarthy), 251 (Christopher Wolf); Software & Info. Indus. Assoc. Comment #00067, *supra* note 2, at 7; Future of Privacy Forum Comment #00027, *supra* note 23, attached report entitled, BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS, at 1–2. See also Lauren Weber, *Can This Algorithm Find Hires of a Certain Race?*, WALL ST. J. (Apr. 30, 2014), <http://blogs.wsj.com/atwork/2014/04/30/can-this-algorithm-find-hires-of-a-certain-race/>.

during interviews. Google then modified its interview practices and began asking more structured behavioral questions (e.g., how would you handle the following situation?).<sup>36</sup> This new approach helped ensure that potential interviewer biases had less effect on hiring decisions.

While recognizing these potential benefits, some researchers and others have expressed concern that the use of big data analytics to make predictions may exclude certain populations from the benefits society and markets have to offer. This concern takes several forms. First, some workshop participants and commenters expressed concerns about the quality of data, including its accuracy, completeness, and representativeness.<sup>37</sup> Another concern is that there are uncorrected biases in the underlying consumer data.<sup>38</sup> For example, one academic has argued that hidden biases in the collection, analysis, and interpretation stages present considerable risks.<sup>39</sup> If the process that generated the underlying data reflects biases in favor of or against certain types of individuals, then some statistical relationships revealed by that data could perpetuate those biases. When not recognized and addressed, poor data quality can lead to inaccurate predictions, which in turn can lead to companies erroneously denying consumers offers or benefits. Although the use of inaccurate or biased data and analysis to justify decisions that have harmed certain populations is not new,<sup>40</sup> some commenters worry that big data analytics may lead to wider propagation of the problem and make it more difficult for the company using such data to identify the source of discriminatory effects and address it.<sup>41</sup>

36 See, e.g., Big Data Tr. 251 (Christopher Wolf). See also Future of Privacy Forum Comment #00027, *supra* note 23, attached report entitled, BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS, at 2; David Amerland, *3 Ways Big Data Changed Google's Hiring Process*, FORBES (Jan. 21, 2014), <http://www.forbes.com/sites/netapp/2014/01/21/big-data-google-hiring-process/>; Adam Bryant, *In Head-Hunting, Big Data May Not Be Such a Big Deal*, N.Y. TIMES (June 19, 2013), <http://www.nytimes.com/2013/06/20/business/in-head-hunting-big-data-may-not-be-such-a-big-deal.html?pagewanted=1&%2359&adxnlnx=1371813584-7rFFVvpSQsf/NlnpuVABGQ&%2359;-r=3>.

37 See, e.g., Big Data Tr. 21–22 (Solon Barocas), 29–31 (David Robinson), 100–02 (Dr. Nicol Turner-Lee); Transcript of Spring Privacy Series: Alternative Scoring Products, in Washington, D.C. (Mar. 19, 2014), at 44–45 (Pamela Dixon) [hereinafter Alternative Scoring Tr.], [https://www.ftc.gov/system/files/documents/public\\_events/182261/alternative-scoring-products\\_final-transcript.pdf](https://www.ftc.gov/system/files/documents/public_events/182261/alternative-scoring-products_final-transcript.pdf). See also Ctr. for Data Innovation Comment #00055, *supra* note 8, attached report entitled, THE RISE OF DATA POVERTY IN AMERICA, at 2; Nat'l Consumer L. Ctr. Comment #00018, *supra* note 1, attached report entitled, Big DATA: A BIG DISAPPOINTMENT FOR SCORING CONSUMER RISK, at 9, 27; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8, at 2. See generally Nir Grinberg et al., *Extracting Diurnal Patterns of Real World Activity from Social Media* (The 9th Int'l Conference on Web and Social Media, Working Paper 2013), <http://sm.rutgers.edu/pubs/Grinberg-SMPatterns-ICWSM2013.pdf>.

38 See, e.g., Big Data Tr. 23–25 (Solon Barocas); Alternative Scoring Tr. 93 (Claudia Perlich). See also Cynthia Dwork & Deirdre Mulligan, *It's Not Privacy and It's Not Fair*, 66 STAN. L. REV. ONLINE 35, 36–37 (2013), <http://www.stanfordlawreview.org/sites/default/files/online/topics/DworkMulliganSLR.pdf>.

39 Kate Crawford, *The Hidden Biases in Big Data*, HARV. BUS. REV. (2013), <https://hbr.org/2013/04/the-hidden-biases-in-big-data>.

40 See generally Helen F. Ladd, *Evidence on Discrimination in Mortgage Lending*, 12(2) J. OF ECON. PERSPECTIVES 41 (1998), [https://www.aeaweb.org/atypon.php?return\\_to=/doi/pdfplus/10.1257/jep.12.2.41](https://www.aeaweb.org/atypon.php?return_to=/doi/pdfplus/10.1257/jep.12.2.41).

41 See, e.g., Big Data Tr. 40–41 (Joseph Turow).

Second, while big data may be highly effective in showing correlations, it is axiomatic that correlation is not causation.<sup>42</sup> Indeed, with large enough data sets, one can generally find some meaningless correlations. For example, in eighteen out of the past twenty U.S. Presidential elections, if the Washington, D.C. professional football team won its last home game before the election, the incumbent's party continued to hold the presidency; if the team lost that last home game, the out-of-office party unseated the incumbent party.<sup>43</sup> Other examples of spurious correlations abound.<sup>44</sup> If companies use correlations to make decisions about people without understanding the underlying reasons for the correlations, those decisions might be faulty and could lead to unintended consequences or harm for consumers and companies.

Ultimately, all of these concerns feed into the larger concern about whether big data may be used to categorize consumers in ways that can result in exclusion of certain populations. Workshop participants and others have noted how potential inaccuracies and biases might lead to detrimental effects for low-income and underserved populations.<sup>45</sup> According to these commenters, particular uses of big data may:

- **Result in more individuals mistakenly being denied opportunities based on the actions of others.** Participants raised concerns that big data can lead to decision-making based on the actions of others with whom consumers share some characteristics.<sup>46</sup> Several commenters explained that some credit card companies have lowered a customer's credit limit, not based on the customer's payment history, but rather based on analysis of other customers with a poor repayment history that had shopped at the same establishments where the customer had shopped.<sup>47</sup> Indeed, one credit card company settled FTC allegations that it failed to disclose its practice of rating consumers as having a greater credit risk because they used their cards to pay for marriage counseling, therapy, or tire-repair services, based on its experiences with other consumers and their repayment histories.<sup>48</sup> Using this type of a statistical model might reduce the cost of credit for some individuals, but may also result

42 See generally John Aldrich, *Correlations Genuine and Spurious in Pearson and Yule*, 10(4) STATISTICAL SCI. 364 (1995), <http://www.jstor.org/stable/2246135>. See also *Correlation*, XKCD, <https://xkcd.com/552/> (last visited Dec. 29, 2015).

43 *Winning Tradition*, SNOPE.COM, <http://www.snopes.com/politics/ballot/redskins.asp> (last visited Dec. 29, 2015).

44 See, e.g., *Spurious Correlations*, TYLERVIGEN.COM, <http://www.tylervigen.com/spurious-correlations> (last visited Dec. 29, 2015) (showing a variety of spurious correlations, including, for example, a historical correlation between the annual number of people who have drowned by falling into a swimming pool and the annual number of films in which Nicolas Cage has appeared).

45 See, e.g., Big Data Tr. 222 (Jeremy Gillula). See generally Nat'l Consumer L. Ctr. Comment #00018, *supra* note 1; Common Sense Media Comment #00016, *supra* note 8; N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8.

46 See, e.g., Big Data Tr. 42–44 (danah boyd). See also Comment #00078 from Seeta Peña Gangadharan et al., New Am.'s Open Tech. Inst., to Fed. Trade Comm'n, attached report entitled, *THE NETWORKED NATURE OF ALGORITHMIC DISCRIMINATION*, at 53–57 (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00078-92938.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00078-92938.pdf).

47 See, e.g., Nat'l Consumer L. Ctr. Comment #00018, *supra* note 1, at 27–28; N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8, at 6.

48 See *FTC v. CompuCredit Corp.*, No. 1:08-cv-1976-BBM-RGV (N.D. Ga. June 10, 2008), <https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081219compucreditsiporder.pdf>. See also Danielle Keats Citron & Frank A. Pasquale III, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 4 (2014), <http://ssrn.com/abstract=2376209>.

in some creditworthy consumers being denied or charged more for credit than they might otherwise have been charged.<sup>49</sup>

- **Create or reinforce existing disparities.** Participants raised concerns that when big data is used to target ads, particularly for financial products, low-income consumers who may otherwise be eligible for better offers may never receive them.<sup>50</sup>
- **Expose sensitive information.** Participants also raised concerns about the potential exposure of characteristics that people may view as sensitive.<sup>51</sup> For example, one study combined data on Facebook “Likes” and limited survey information to determine that researchers could accurately predict a male user’s sexual orientation 88 percent of the time; a user’s ethnic origin 95 percent of the time; and whether a user was Christian or Muslim (82 percent), a Democrat or Republican (85 percent), or used alcohol, drugs, or cigarettes (between 65 percent and 75 percent).<sup>52</sup>
- **Assist in the targeting of vulnerable consumers for fraud.** Unscrupulous companies can use big data to offer misleading offers or scams to the most vulnerable prospects.<sup>53</sup> According to public reports, unscrupulous companies can obtain lists of people who reply to sweepstakes offers and thus are more likely to respond to enticements, as well as lists of “suffering seniors” who are identified as having Alzheimer’s or similar maladies.<sup>54</sup> Big data analytics allows companies to more easily and accurately identify such vulnerable prospects.
- **Create new justifications for exclusion.** Big data analytics may give companies new ways to attempt to justify their exclusion of certain populations from particular opportunities. For example, one big data analytics study showed that “people who fill out online job applications using browsers that did not come with the computer . . . but had to be deliberately installed (like Firefox or Google’s

49 See, e.g., Alternative Scoring Tr. 96 (Edmund Mierzwinski).

50 See, e.g., Big Data Tr. 228–30 (Christopher Calabrese); Alternative Scoring Tr. 64–67 (Ashkan Soltani). See also Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8, at 10–11, 18–29.

51 See, e.g., Big Data Tr. 89–90 (Pamela Dixon), 71–72 (Kristin Amerling); Alternative Scoring Tr. 76 (Pamela Dixon), 92 (Ashkan Soltani). See also Am.’s Open Tech. Inst. Comment #00078, *supra* note 46, attached report entitled, HEALTH PRIVACY ONLINE: PATIENTS AT RISK, at 11–16; Ctr. on Privacy & Tech. at Geo. L. Comment #00024, *supra* note 8, at 9; DATA BROKERS REPORT, *supra* note 7, at 19–21, 47.

52 See Michal Kosinski et al., *Private Traits and Attributes Are Predictable From Digital Records of Human Behavior*, 110 PROCEEDINGS OF THE NAT’L ACAD. OF SCI. 5802, 5803–04 (2013), <http://www.pnas.org/content/110/15/5802.abstract>. See also Jon Green, *Facebook Knows You’re Gay Before You Do*, AM. BLOG (Mar. 20, 2013), <http://americablog.com/2013/03/facebook-might-know-youre-gay-before-you-do.html>.

53 See, e.g., Comment #00080 from David Robinson, Robinson + Yu, to Fed. Trade Comm’n 8–9 (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00080-92939.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00080-92939.pdf); N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8, at 6–7. See also FTC v. LeapLab, LLC, No. 2:14-cv-02750 (D. Ariz. filed Dec. 22, 2014), <https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf>.

54 See, e.g., N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8, at 6–7.

Chrome) perform better and change jobs less often.”<sup>55</sup> If an employer were to use this correlation to refrain from hiring people who used a particular browser, they could be excluding qualified applicants for reasons unrelated to the job at issue.

- **Result in higher-priced goods and services for lower income communities.** Some commentators have raised concerns about potential effects on prices on lower income communities.<sup>56</sup> For example, research has shown that online companies may charge consumers in different zip codes different prices for standard office products.<sup>57</sup> If such pricing results in consumers in poorer neighborhoods having to pay more for online products than consumers in affluent communities, where there is more competition from brick-and-mortar stores, these poorer communities would not realize the full competition benefit of online shopping.<sup>58</sup>
- **Weaken the effectiveness of consumer choice.** Some researchers have argued that, even when companies offer consumers choices about data collection, the companies may still use big data to draw inferences about consumers who choose to restrict the collection of their data.<sup>59</sup> Indeed, using data from consumers who opt in or decline to opt out, big data algorithms can still be employed to infer information about similarly-situated individuals who chose not to share their data.<sup>60</sup>

55 See, e.g., Mark Andrejevic, *The Big Data Divide*, 8 INT'L J. OF COMM'N 1673, 1681 (2014), <http://ijoc.org/index.php/ijoc/article/download/2161/1163>. See also *Robot Recruiters*, ECONOMIST (Apr. 6, 2013), <http://www.economist.com/news/business/21575820-how-software-helps-firms-hire-workers-more-efficiently-robot-recruiters>.

56 See, e.g., Lauren Kirchner, *When Big Data Becomes Bad Data*, PROPUBLICA (Sept. 2, 2015), <https://www.propublica.org/article/when-big-data-becomes-bad-data> (finding that areas with high density of Asian residents are often charged more for the Princeton Review's online SAT tutoring). But see EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND DIFFERENTIAL PRICING 17 (2015), [hereinafter WHITE HOUSE FEB. 2015 REPORT], [http://www.whitehouse.gov/sites/default/files/whitehouse\\_files/docs/Big\\_Data\\_Report\\_Nonembargo\\_v2.pdf](http://www.whitehouse.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf) (“[I]f historically disadvantaged groups are more price-sensitive than the average consumer, profit-maximizing differential pricing should work to their benefit” in competitive markets.). This holds true for relatively competitive markets. However, the report also points out that disadvantaged groups may face less competitive markets and be penalized by differential pricing. *Id.* Economists have shown that price discrimination can improve or reduce consumer welfare, depending on how price discrimination is implemented. See generally Dirk Bergemann et al., *The Limits of Price Discrimination*, 105(3), AM. ECON. REV. 921 (2015), <https://www.aeaweb.org/articles.php?doi=10.1257/aer.20130848>. Economists have also shown that greater price discrimination could raise or reduce the intensity of competition. See generally Kenneth S. Cortis, *Third-Degree Price Discrimination in Oligopoly: All-Out Competition and Strategic Commitment*, RAND J. OF ECON. 306 (1998), [http://www.jstor.org/stable/2555890?seq=1#page\\_scan\\_tab\\_contents](http://www.jstor.org/stable/2555890?seq=1#page_scan_tab_contents).

57 See, e.g., Alternative Scoring Tr. 62–64 (Ashkan Soltani). See also Jennifer Valentino-Devries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), <http://www.wsj.com/articles/SB10001424127887323777204578189391813881534>.

58 See, e.g., Nat'l Consumer L. Ctr Comment #00018, *supra* note 1, at 27; N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8, at 4–5. See also Alternative Scoring Tr. 62–64 (Ashkan Soltani). For an example of differential pricing using IP addresses, see Valentino-Devries et al., *supra* note 57. For an example of steering based on the type of operating system, see Martha C. White, *Orbitz Shows Higher Prices to Mac Users*, TIME (June 26, 2012), <http://business.time.com/2012/06/26/orbitz-shows-higher-prices-to-mac-users/>.

59 Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, in *PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT* 44, 61–63 (Julia Lane et al. eds., 2014).

60 *Id.*

As these examples show, big data offers companies the opportunity to facilitate inclusion or exclusion. Companies can use big data to advance education, credit, and employment opportunities for low-income communities or to exclude them from these opportunities. They can use big data to target products to those who are most interested or to target products in ways that could exclude certain populations. The remainder of this report is intended to guide companies on some of the laws that may apply when using big data, raise awareness about the ethical implications of using big data, and to highlight potential biases that companies should consider as they use big data.

## IV. Considerations for Companies in Using Big Data

The challenge for companies is not *whether* they should use big data; indeed, the reality of today's marketplace is that big data now fuels the creation of innovative products and systems that consumers and companies quickly are coming to rely upon and expect. Rather, the challenge is *how* companies can use big data in a way that benefits them and society, while minimizing legal and ethical risks.

In assessing risks, companies should first have an understanding of the laws that may apply to big data practices. Second, they should be aware of important research in the field of big data aimed at identifying potential biases and inaccuracies. This section provides a starting point for companies using big data analytics. It is not intended to provide an exhaustive list of considerations. Rather, companies using big data should consider the issues raised in this report as they engage in big data practices and build on the questions posed to examine the legal, privacy, and ethical implications of their work.

### A. Potentially Applicable Laws

The following section describes some of the laws that may apply to big data practices.<sup>61</sup> Although the laws discussed do not address every potential misuse, as noted above, this report is not intended to identify

61 See, e.g., Big Data Tr. 38 (Kristin Amerling), 45–47, 69–70 (David Robinson), 95, 120–22 (Stuart Pratt), 99, 108 (Pamela Dixon), 268 (Christopher Calabrese), 163–213 (Leonard Chanin, Carol Miaskoff, Montserrat Miller, C. Lee Peeler, and Peter Swire in conversation); Alternative Scoring Tr. 36–37, 71 (Stuart Pratt). See generally Comment #00075 from Michelle De Mooy, Ctr. for Democracy & Tech., to Fed. Trade Comm'n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00075-92928.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00075-92928.pdf); Comment #00068 from Julie Kearney & Alexander Reynolds, Consumer Elecs. Assoc., to Fed. Trade Comm'n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00068-92917.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00068-92917.pdf); Software & Info. Indus. Assoc. Comment #00067, *supra* note 2; Future of Privacy Forum Comment #00065, *supra* note 2; Direct Mktg. Assoc. Comment #00063, *supra* note 23; Comment #00062 from David Hoffman, Intel Corp., to Fed. Trade Comm'n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00062-92887.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00062-92887.pdf); Comment #00061 from Jeff Chester, Ctr. for Dig. Democracy, & Edmund Mierzwinski, U.S. PIRG Educ. Fund, to Fed. Trade Comm'n (Oct. 29, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00061-92886.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00061-92886.pdf); Comment #00059 from Laura Murphy & Rachel Goodman, Am. Civil Liberties Union, to Fed. Trade Comm'n (Oct. 27, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00059-92874.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00059-92874.pdf); Ctr. for Data Innovation Comment #00026, *supra* note 8; Comment #00025 from Dennis Hirsch, Cap. Univ. L. Sch., to Fed. Trade Comm'n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00025-92435.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00025-92435.pdf); Comment #00021 from U.S. Chamber of Commerce, to Fed. Trade Comm'n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00021-92389.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00021-92389.pdf); Comment #00020 from Jim Halpert, Internet Commerce Coal., to Fed. Trade Comm'n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00020-92388.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00020-92388.pdf).

legal or policy gaps; rather, it attempts to guide companies on laws, such as the Fair Credit Reporting Act, equal opportunity laws, and the Federal Trade Commission Act, that may apply to big data practices.<sup>62</sup>

### 1. The Fair Credit Reporting Act

The FTC has the authority to enforce compliance with the Fair Credit Reporting Act (“FCRA”).<sup>63</sup> The FCRA applies to companies, known as consumer reporting agencies or CRAs, that compile and sell consumer reports, which contain consumer information that is used or expected to be used for credit, employment, insurance, housing, or other similar decisions about consumers’ eligibility for certain benefits and transactions.<sup>64</sup> Among other things, CRAs must implement reasonable procedures to ensure maximum possible accuracy of consumer reports<sup>65</sup> and provide consumers with access to their own information, along with the ability to correct any errors.<sup>66</sup> CRAs can only provide consumer reports to those entities that will use them for certain specified permissible purposes, such as for credit, employment, insurance, or housing eligibility determinations.<sup>67</sup>

Traditionally, CRAs include credit bureaus, employment background screening companies, and other specialty companies that provide particularized services for making consumer eligibility decisions, such as check authorizations or tenant screenings. Some data brokers that compile non-traditional information, including social media information, may also be considered CRAs subject to the FCRA, as demonstrated by the Commission’s enforcement actions. For example, the Commission entered into a consent decree with online data broker Spokeo to resolve allegations that the company violated the FCRA.<sup>68</sup> As set forth in the FTC’s complaint, Spokeo assembled personal information from hundreds of online and offline data sources, including social networks, and merged that data to create detailed personal profiles, including name, address, age range, hobbies, ethnicity, and religion, and marketed these profiles for use by human resources

---

[www.ftc.gov/system/files/documents/public\\_comments/2014/08/00020-92376.pdf](http://www.ftc.gov/system/files/documents/public_comments/2014/08/00020-92376.pdf); Comment #00019 from Michael Beckerman, Internet Ass’n, to Fed. Trade Comm’n (Aug. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/08/00019-92375.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/08/00019-92375.pdf); Nat’l Consumer L. Ctr. Comment #00018, *supra* note 1; Interactive Advert. Bureau Comment #00017, *supra* note 23; World Privacy Forum Comment #00014, *supra* note 19; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8.

62 This discussion articulates considerations relevant to the Commission’s exercise of its enforcement authority. Though this section discusses certain federal laws, companies should also be aware that other federal laws, as well as state and local laws, may apply to their big data practices. They should review these laws in jurisdictions where they operate.

63 15 U.S.C. §§ 1681–1681x (2014).

64 *Id.* § 1681a(f) & (d). As discussed further below, the FCRA also applies to users of consumer reports and those who furnish consumer reports to CRAs.

65 *Id.* § 1681e(b).

66 *Id.* § 1681g–1681j.

67 *Id.* § 1681b(a).

68 *United States v. Spokeo, Inc.*, No. 2-12-cv-05001-MMM-SH (C.D. Cal. June 12, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeoorder.pdf>. See also Press Release, Fed. Trade Comm’n, Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA (June 12, 2012), <http://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftccharges-company-allegedly-marketed>.



departments in making hiring decisions.<sup>69</sup> Based on the allegations that the company marketed consumer profiles specifically for employment purposes, the Commission charged that Spokeo was subject to, but had failed to comply with, the FCRA. Accordingly, the FTC entered into a consent decree that required Spokeo to pay \$800,000 in civil penalties.

In another matter, the Commission alleged that the data broker Instant Checkmate advertised potential uses of its consumer data for employment and tenant screening purposes, both through its website and through blog posts, but did not comply with the FCRA.<sup>70</sup> According to the complaint, the company used a Google AdWords campaign to display ads for its services that would appear in search results when consumers sought background checks on “nannies,” “babysitters,” “maids,” and “housekeepers.” Thus, the Commission alleged that the company was subject to the FCRA, entered into a consent order to ensure future compliance, and obtained \$550,000 in civil penalties.<sup>71</sup> In both *Spokeo* and *Instant Checkmate*, the companies included a disclaimer on their websites stating that they were not CRAs and that users could not use their data for eligibility purposes. These disclaimers were not effective in insulating the companies from FTC enforcement. As these cases demonstrate, the scope of the FCRA extends beyond traditional credit bureaus.

Companies that use consumer reports also have obligations under the FCRA. They must, among other things, provide consumers with “adverse action” notices if the companies use the consumer report information to deny credit, insurance, employment, housing, or certain other covered benefits.<sup>72</sup> Similarly, companies that use consumer reports must provide “risk-based pricing” notices if they charge consumers more to obtain credit or insurance based on consumer report information.<sup>73</sup> The purpose of both types of notices is to enable consumers to check their consumer reports and correct any inaccuracies.<sup>74</sup> The Commission has brought actions against various companies for violation of these provisions.<sup>75</sup> For example,

69 Complaint at 3–4, *Spokeo*, No. 2:12-cv-05001-MMM-SH (C.D. Cal. filed June 7, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120612spokeocmpt.pdf>.

70 Complaint, United States v. Instant Checkmate, Inc., No. 3:14-cv-00675-H-JMA (S.D. Cal. filed Mar. 24, 2014), <https://www.ftc.gov/system/files/documents/cases/140409instantcheckmatecmpt.pdf>. See also Press Release, Fed. Trade Comm’n, Two Data Brokers Settle FTC Charges That They Sold Consumer Data without Complying with Protections Required under the Fair Credit Reporting Act (Apr. 9, 2014), <https://www.ftc.gov/news-events/press-releases/2014/04/two-data-brokers-settle-ftc-charges-they-sold-consumer-data>.

71 *Instant Checkmate*, No. 3:14-cv-00675-H-JMA (S.D. Cal. Apr. 1, 2014), <https://www.ftc.gov/system/files/documents/cases/140409instantcheckmateorder.pdf>.

72 See 15 U.S.C. § 1681m(a). When using consumer reports for employment purposes, companies must also provide consumers with “pre-adverse action notices” before taking any adverse action. See *id.* § 1681b(b)(3).

73 See *id.* § 1681m(h); 12 C.F.R. §§ 1022.70–1022.75 (2015); FTC Duties of Creditors Regarding Risk-Based Pricing Rule, 16 C.F.R. § 640 (2015).

74 See *Using Consumer Reports for Credit Decisions: What to Know About Adverse Action and Risk-Based Pricing Notices*, FED. TRADE COMM’N (Dec. 2013), <https://www.ftc.gov/tips-advice/business-center/guidance/using-consumer-reports-credit-decisions-what-know-about-adverse>.

75 See, e.g., Complaint, United States v. Rail Terminal Servs., LLC, No. 09-cv-1111(MJP) (W.D. Wash. filed Aug. 11, 2009), <https://www.ftc.gov/sites/default/files/documents/cases/2013/08/090806trscmpt.pdf>; Complaint, United States v. Quality

in 2013, the FTC brought an action against Time Warner Cable because it used a consumer report to determine whether to require deposits on consumers' cable bills.<sup>76</sup> The complaint alleged that consumers who were charged a deposit should have received a risk-based pricing notice informing them that the charge was based on information in their consumer report. The consent order barred Time Warner Cable from future violations of the Risk-Based Pricing Rule and required the company to pay \$1.9 million in civil penalties.<sup>77</sup> In addition, in 2015, the Commission brought an action against Sprint alleging that the company failed to give proper risk-based pricing notices to consumers who were placed in a program for customers with lower credit scores and charged an extra monthly fee.<sup>78</sup> The consent order requires Sprint to pay a \$2.95 million penalty and to give timely notice to consumers placed in such a program.<sup>79</sup>

The FCRA, however, does not apply to companies when they use data derived from their own relationship with their customers for purposes of making decisions about them.<sup>80</sup> But if an unaffiliated firm regularly evaluates companies' own data and provides the evaluations to the companies for eligibility determinations, the unaffiliated firm would likely be acting as a CRA, each company would likely be a user of consumer reports, and all of these entities would be subject to Commission enforcement under the FCRA.

Workshop panelists and commenters discussed a growing trend in big data, in which companies may be purchasing predictive analytics products for eligibility determinations.<sup>81</sup> Under traditional credit scoring

---

Terminal Servs., LLC, No. 09-cv-01853-CMA-BNB (D. Colo. filed Aug. 11, 2009), <https://www.ftc.gov/sites/default/files/documents/cases/2009/08/090806ptscmpt.pdf>.

76 Complaint, United States v. Time Warner Cable, Inc., No. 13-cv-8998 (S.D.N.Y. filed Dec. 19, 2013), <https://www.ftc.gov/sites/default/files/documents/cases/131219timewarnercmpt.pdf>. See also Press Release, Fed. Trade Comm'n, Time Warner Cable to Pay \$1.9 Million Penalty for Violating Risk-Based Pricing Rule (Dec. 19, 2013), <https://www.ftc.gov/news-events/press-releases/2013/12/time-warner-cable-pay-19-million-penalty-violating-risk-based>.

77 *Time Warner Cable*, No. 13-cv-8998 (S.D.N.Y. Dec. 20, 2013), <https://www.ftc.gov/sites/default/files/documents/cases/131219timewarnerstip.pdf>.

78 Complaint at 7–8, United States v. Sprint Corp., No. 2:15-cv-9340 (D. Kan. filed Oct. 21, 2015), <https://www.ftc.gov/system/files/documents/cases/151021sprintcmpt.pdf>. See also Press Release, Fed. Trade Comm'n, Sprint Will Pay \$2.95 Million Penalty to Settle FTC Charges It Violated Fair Credit Reporting Act (Oct. 21, 2015), <https://www.ftc.gov/news-events/press-releases/2015/10/sprint-will-pay-295-million-penalty-settle-ftc-charges-it>.

79 The settlement also requires Sprint to send corrected risk-based pricing notices to consumers who received incomplete notices from the company. See *Sprint*, No. 2:15-cv-9340 (D. Kan. Oct. 21, 2015), <https://www.ftc.gov/system/files/documents/cases/151021sprintstip.pdf>.

80 15 U.S.C. § 1681a(d)(2)(A)(i). See also FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 1, 23–24 (2011) [hereinafter 40 YEARS FCRA REPORT], <https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcraareport.pdf> ("Reports limited to transactions or experiences between the consumer and the entity making the report are not consumer reports. An opinion that is based only on transactions or experiences between the consumer and the reporting entity is also within the exception.")

81 See, e.g., Big Data Tr. 38 (Kristin Amerling), 69–70 (David Robinson), 99–100 (Pamela Dixon); Alternative Scoring Tr. 100–101 (Pamela Dixon). See also Nat'l Consumer L. Ctr. Comment #00018, *supra* note 1, at 20–23; World Privacy Forum Comment #00014, *supra* note 19, at 19–21; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8, at 13–15; Comment #00006 from Jeff Chester, Ctr. for Dig. Democracy, & Edmund Mierzwinski,

models, companies compare known credit characteristics of a consumer—such as past late payments—with historical data that shows how people with the same credit characteristics performed over time in meeting their credit obligations. Similarly, predictive analytics products may compare a known characteristic of a consumer to other consumers with the same characteristic to predict whether that consumer will meet his or her credit obligations. The difference is that, rather than comparing a traditional credit characteristic, such as debt payment history, these products may use non-traditional characteristics—such as a consumer’s zip code, social media usage, or shopping history—to create a report about the creditworthiness of consumers that share those non-traditional characteristics, which a company can then use to make decisions about whether that consumer is a good credit risk.<sup>82</sup> The standards applied to determine the applicability of the FCRA, however, are the same.

In exercising its enforcement authority, the Commission looks to the FCRA’s definition of a “consumer report.” The FCRA defines a consumer report as a communication from a CRA (1) bearing on a consumer’s personal characteristics or mode of living<sup>83</sup> (2) that “is used or expected to be used . . . for the purpose of serving as a factor in establishing the consumer’s eligibility.”<sup>84</sup> Under this definition, the communication must be prepared or provided to others to make an eligibility determination about a particular consumer.

Suppose a company asks a consumer to provide her zip code and information about her social media and shopping behavior on a credit application, strips the consumer’s identifying information, and sends the application to an analytics firm. The firm then analyzes the creditworthiness of people in the same zip code with similar social media and shopping behaviors as the consumer and provides that analysis—be it, for example, in the form of a score, a grade, or a recommendation—to the company, knowing that it is to be used for a credit decision. Because the company is using information about the consumer to generate an analysis of a group that shares some characteristics with the consumer and then is using that analysis to make a decision about the consumer, the Commission would likely regard the analysis to be a consumer report, and FCRA requirements and protections would likely apply.<sup>85</sup>

---

U.S. PIRG Educ. Fund. to Fed. Trade Comm’n (Mar. 18, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/03/00006-89085.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/03/00006-89085.pdf).

82 See, e.g., Big Data Tr. 69–70 (David Robinson) (noting that these “thinly aggregated scores . . . may be used to lower [consumers’] credit limits”); 99–100 (Pamela Dixon) (noting that these scores are “problematic for ensuring privacy and fairness” because they rely on “[un]regulated data”); Alternative Scoring Tr. 94 (Pamela Dixon) (describing “cohort scoring,” which is a type of score based on a consumer’s social media friends). See also World Privacy Forum Comment #00014, *supra* note 19, at 32–38. But see *supra* text accompanying notes 27–30 (explaining how big data analytics can be used to expand credit availability).

83 As noted in *Trans Union Corp. v. FTC*, this part of the test is not a very demanding one, for almost any information about consumers arguably bears on their personal characteristics or mode of living. 81 F.3d 228, 231 (D.C. Cir. 1996).

84 15 U.S.C. § 1681a(d)(1) (emphasis added).

85 In 2011, FTC staff issued the 40 YEARS FCRA REPORT. In that report, staff stated that “[i]nformation that does not identify a specific consumer does not constitute a consumer report even if the communication is used in part to determine eligibility.” 40 YEARS FCRA REPORT, *supra* note 80, at 20. The Commission does not believe that this statement is accurate. If a report is crafted for eligibility purposes with reference to a particular consumer or set of particular consumers (e.g., those that have

In contrast, if a company uses an analytics firm's report simply to inform its general policies, then the Commission would likely not regard the report to be a consumer report under the FCRA because such a general report does not relate to a particular consumer. For example, if an analytics firm's report simply provides an "aggregate credit score" for every zip code in the United States, a company finds the report through a search engine, and the company uses the report to inform its policies, the Commission would likely not consider the analytics firm's report to be a consumer report or the analytics firm to be a CRA.<sup>86</sup>

As noted above, it is well settled under the FCRA that when a company denies a consumer credit, or charges a higher price for credit, based on information from a CRA, the company must provide the consumer with an adverse action notice. But a creditor may still have obligations under the FCRA even in cases where the creditor obtains information from a company other than a CRA. Section 615(b) of the FCRA provides that, when a company denies a consumer credit, or charges a higher price for credit, based on information from a person *other than a CRA*, the consumer may request, in writing, that the company disclose to him or her the nature of the information leading to the denial or increase in charge.<sup>87</sup> Thus, continuing with the example above, even if a store finds a general analytics company report through a search engine and then uses the report to inform its credit granting policies, the store would have to disclose the nature of the report upon the consumer's request if the consumer's application for credit is denied or the charge for such credit is increased as a result of reliance on the report.

Only a fact-specific analysis will ultimately determine whether a practice is subject to or violates the FCRA, and as such, companies should be mindful of the law when using big data analytics to make FCRA-covered eligibility determinations.

## 2. Equal Opportunity Laws

When engaging in big data analytics, companies should also consider federal equal opportunity laws, including the Equal Credit Opportunity Act ("ECOA"),<sup>88</sup> Title VII of the Civil Rights Act of 1964,<sup>89</sup>

---

applied for credit), the Commission will consider the report a consumer report even if the identifying information of the consumer has been stripped.

86 Companies that determine eligibility based on zip codes should exercise caution. Such a practice could still implicate equal opportunity laws, if that policy has a disproportionate adverse effect or impact on a protected class, unless those practices or policies further a legitimate business need that cannot reasonably be achieved by means that are less disproportionate in their impact. See discussion *infra* Part IV.A.2.

87 See 15 U.S.C. § 1681m(b).

88 15 U.S.C. §§ 1691 *et seq.* (2014). In addition to prohibiting discrimination, ECOA and Regulation B include other requirements that may be implicated by business practices that utilize big data analytics. Informing credit applicants about adverse actions related to applications for credit and identifying the specific reasons an adverse action was taken may be challenging when those reasons implicate big data analytics. See 12 C.F.R. § 1002.9. Lenders may also need to review Regulation B requirements on how information is obtained and retained in the credit application process. See 12 C.F.R. § 1002.5(b)–(d), 1002.12(a)(2).

89 42 U.S.C. §§ 2000e *et seq.* (2014). The Civil Rights Act of 1964 also applies to education, voting, and public accommodations.

the Americans with Disabilities Act,<sup>90</sup> the Age Discrimination in Employment Act (“ADEA”),<sup>91</sup> the Fair Housing Act (“FHA”),<sup>92</sup> and the Genetic Information Nondiscrimination Act (“GINA”).<sup>93</sup> These laws prohibit discrimination based on protected characteristics such as race, color, sex or gender, religion, age, disability status, national origin, marital status, and genetic information.<sup>94</sup>

Companies should review these laws and take steps to ensure their use of big data analytics complies with the discrimination prohibitions that may apply. This section discusses some examples of relevant considerations under these laws related to employment and credit, as highlighted in the workshop.

To prove a violation of federal equal credit or employment opportunity laws, plaintiffs typically must show “disparate treatment” or “disparate impact.”<sup>95</sup> Disparate treatment occurs when an entity, such as a creditor or employer, treats an applicant differently based on a protected characteristic such as race or national origin.<sup>96</sup> Systemic disparate treatment occurs when an entity engages in a pattern or practice of differential treatment on a prohibited basis.<sup>97</sup> In some cases, the unlawful differential treatment could be based on big data analytics.<sup>98</sup> For example, an employer may not disfavor a particular protected group because big data analytics show that members of this protected group are more likely to quit their jobs within a five-year period.<sup>99</sup> Similarly, a lender cannot refuse to lend to single persons or offer less favorable terms to them than married persons even if big data analytics show that single persons are less likely to repay loans than married persons. Evidence of such violations could include direct evidence of the reasons for the company’s choices, or circumstantial evidence, such as significant statistical disparities in outcomes for protected groups that are unexplained by neutral factors.

<sup>90</sup> 42 U.S.C. §§ 12101 *et seq.* (2014).

<sup>91</sup> 29 U.S.C. §§ 621 *et seq.* (2014).

<sup>92</sup> 42 U.S.C. §§ 3601 *et seq.* (2014).

<sup>93</sup> 42 U.S.C. §§ 2000ff *et seq.* (2014). GINA also applies to health insurance.

<sup>94</sup> A number of different agencies have the authority to enforce the various equal opportunity laws. The Equal Employment Opportunity Commission, for example, is responsible for enforcing Title VII of the Civil Rights Act of 1964 (along with the Department of Justice (“DOJ”)), the Age Discrimination in Employment Act of 1967, and GINA. The Department of Housing and Urban Development and the DOJ enforce the FHA. The FTC, DOJ, and the Consumer Financial Protection Bureau (“CFPB”), among other agencies, enforce ECOA and its implementing Regulation B.

<sup>95</sup> See, e.g., Big Data Tr. 168–170 (Carol Miaskoff). Disparate impact claims are not permitted under Title II of GINA. *Background Information for EEOC Notice of Proposed Rulemaking on Title II of the Genetic Information Nondiscrimination Act of 2008*, U.S. EQUAL EMP’T OPPORTUNITY COMM’N, [http://www.eeoc.gov/policy/docs/qanda\\_geneticinfo.html](http://www.eeoc.gov/policy/docs/qanda_geneticinfo.html) (last modified May 12, 2009).

<sup>96</sup> See, e.g., 29 U.S.C. § 623(a)(1); 42 U.S.C. § 2000e–2(k)(1)(A)(i); 42 U.S.C. § 12112(b)(1); 12 C.F.R. Part 1002 Supp. I § 1002.4(a)–1.

<sup>97</sup> See, e.g., *Int’l Bhd. of Teamsters v. United States*, 431 U.S. 324, 334–35 (1977).

<sup>98</sup> See, e.g., Big Data Tr. 168–170 (Carol Miaskoff).

<sup>99</sup> *Cf. id.* (explaining how the various equal opportunity laws may apply to big data analytics).

Practices that have a “disparate impact” on protected classes may also violate equal credit or employment opportunity laws.<sup>100</sup> While specific disparate impact standards vary depending on the applicable law, in general, disparate impact occurs when a company employs facially neutral policies or practices that have a disproportionate adverse effect or impact on a protected class,<sup>101</sup> unless those practices or policies further a legitimate business need<sup>102</sup> that cannot reasonably be achieved by means that have less disparate an impact.<sup>103</sup>

Disparate impact analysis has important implications for big data.<sup>104</sup> Under such an analysis, a company that avoids, for example, expressly screening job applicants based on gender and instead uses big data analytics to screen job applicants in a way that has a disparate impact on women may still be subject to certain equal employment opportunity laws, if the screening does not serve a legitimate business need or if the need can reasonably be achieved by another means with a smaller disparate impact.<sup>105</sup> Likewise, if a company makes credit decisions based on zip codes, it may be violating ECOA if the decisions have a disparate impact on a protected class and are not justified by a legitimate business necessity.<sup>106</sup> Even if evidence shows the decisions are justified by a business necessity, if there is a less discriminatory alternative, the decisions may still violate ECOA.<sup>107</sup>

100 See, e.g., 29 U.S.C. § 631(a); 42 U.S.C. § 2000e–2 (k); 42 U.S.C. § 12112(b)(6); 24 C.F.R. § 100.500; 12 C.F.R. Part 1002 Supp. I § 1002.6(a)–2. On June 25, 2015, the Supreme Court in *Texas Department of Housing and Community Affairs v. Inclusive Communities Project, Inc.*, 135 S.Ct. 2507 (2015), held that the disparate impact theory is valid under the FHA.

101 See, e.g., 12 C.F.R. § 1002.6 (citing *Griggs v. Duke Power Co.*, 401 U.S. 424 (1971), and *Albermarle Paper Co. v. Moody*, 422 U.S. 405, 430–31 (1975)); 12 C.F.R. Part 1002 Supp. I § 1002.6(a)–2; Policy Statement on Discrimination in Lending, 59 Fed. Reg. 18,266, 18,268 (Apr. 14, 1994).

102 See, e.g., *Tex. Dep’t of Cmty. Affairs v. Burdine*, 450 U.S. 248, 256–58 (1981); *N.Y. City Transit Auth. v. Beazer*, 440 U.S. 568, 587 (1979); *Zamlen v. City of Cleveland*, 906 F.2d 209, 218–20 (6th Cir. 1990); *Evans v. City of Evanston*, 881 F.2d 382, 383 (7th Cir. 1989); *Aguilera v. Cook County Police & Corr. Merit Bd.*, 760 F.2d 844, 846–47 (7th Cir. 1985). See also 12 C.F.R. § 1002.6(a). However, with respect to ADEA cases, the formulation applied by courts is slightly different. See, e.g., *Smith v. City of Jackson*, 544 U.S. 228, 243 (2005) (holding that the “reasonable factor other than age” test, rather than the business necessity test, is the appropriate standard for determining lawfulness of a practice that disproportionately affects older workers under the ADEA). See also *Questions and Answers on EEOC Final Rule on Disparate Impact and “Reasonable Factors Other Than Age” Under the Age Discrimination Employment Act of 1967*, U.S. EQUAL EMP’T OPPORTUNITY COMM’N, [http://www.eeoc.gov/laws/regulations/adea\\_rfoa\\_qa\\_final\\_rule.cfm](http://www.eeoc.gov/laws/regulations/adea_rfoa_qa_final_rule.cfm) (last visited on Dec. 28, 2015).

103 See, e.g., *Albermarle Paper*, 422 U.S. at 425; *Int’l Bhd. of Elec. Workers, AFL-CIO, Local Unions Nos. 605 & 985 v. Miss. Power & Light Co.*, 442 F.3d 313, 318–19 (5th Cir. 2006); *Smith v. City of Des Moines, Iowa*, 99 F.3d 1466, 1473 (8th Cir. 1996); *Contreras v. City of Los Angeles*, 656 F.2d 1267, 1285 (9th Cir. 1981); *El v. Se. Pa. Transp. Auth.*, 418 F. Supp. 2d 659, 672 (E.D. Pa. 2005) *aff’d*, 479 F.3d 232 (3d Cir. 2007).

104 Big data can also facilitate the identification of disparate impact. See *infra* notes 145–47 and accompanying text.

105 See, e.g., *Big Data Tr.* 170 (Carol Miaskoff).

106 The use of zip codes can also raise concerns of redlining, a form of discrimination involving differential treatment on the basis of the race, color, national origin, or other protected characteristic of residents of those areas in which the credit seeker resides, or will reside, or in which residential property to be mortgaged is located. The CFPB and DOJ recently concluded a redlining enforcement action against Hudson City Savings Bank. See Complaint, CFPB v. Hudson City Sav. Bank, No. 15-07056 (D.N.J. Sept. 24, 2015), [http://files.consumerfinance.gov/f/201509\\_cfpb\\_hudson-city-joint-complaint.pdf](http://files.consumerfinance.gov/f/201509_cfpb_hudson-city-joint-complaint.pdf). See also CONSUMER FIN. PROTECTION BUREAU, CFPB EXAMINATION PROCEDURES: ECOA BASELINE REVIEW MODULES 16–18 (2013), [http://files.consumerfinance.gov/f/201307\\_cfpb\\_ecoa\\_baseline-review-module-fair-lending.pdf](http://files.consumerfinance.gov/f/201307_cfpb_ecoa_baseline-review-module-fair-lending.pdf).

107 The examples above are illustrative and do not necessarily provide an exhaustive list of all ways that big data could have a disparate impact on consumers.

The FTC's enforcement actions include dozens of consent orders resolving alleged violations of ECOA. Some of these cases have been based on a disparate treatment theory. For example, ECOA prohibits discrimination against applicants who are receiving public assistance.<sup>108</sup> The Commission has brought cases against lenders that allegedly excluded public assistance income in deciding whether to extend credit.<sup>109</sup> Likewise, ECOA prohibits discounting or refusing to consider income on the basis of marital status.<sup>110</sup> The FTC has brought cases against lenders that allegedly failed to aggregate the income of unmarried joint applicants, while combining incomes for applicants who were married.<sup>111</sup>

The FTC also has alleged discrimination under a disparate impact legal standard under ECOA. For example, the FTC settled two cases alleging that lenders failed to appropriately monitor loan officers whose mortgage loans resulted in minority applicants' being charged higher prices than non-Latino white applicants.<sup>112</sup> The Commission alleged that the statistically significant pricing disparities could not be explained by any legitimate underwriting risk factors or credit characteristics of the applicants.

Workshop discussions focused in particular on whether advertising could implicate equal opportunity laws.<sup>113</sup> For example, suppose big data analytics show that single women are more likely to apply for subprime credit products. Would targeting advertisements for these products to single women violate ECOA?<sup>114</sup> Certainly, prohibiting single women from applying for a prime credit card based on their marital status would violate ECOA.<sup>115</sup> But what if a single woman would qualify for the prime product, but because of big data analytics, the subprime product with a higher interest rate is the only one advertised to her?

In most cases, a company's advertisement to a particular community for a credit offer that is open to all to apply is unlikely, by itself, to violate ECOA, absent disparate treatment or an unjustified disparate

---

108 15 U.S.C. § 1691(a)(2).

109 *See, e.g.*, Complaint, United States v. Franklin Acceptance Corp., No. 99-cv-2435 (E.D. Penn. filed May 13, 1999), <https://www.ftc.gov/sites/default/files/documents/cases/1999/05/franklincomp.htm>.

110 15 U.S.C. § 1691(a)(1).

111 *See, e.g.*, Complaint, United States v. Ford Motor Credit Co., No. 99-cv-57887 (GEW) (E.D. Mich. filed Dec. 9, 1999), <https://www.ftc.gov/sites/default/files/documents/cases/1999/12/fordmotorcompanyfederalcourtcomplaint.pdf>.

112 *See* Complaint, FTC v. Gateway Diversified Funding Mortg. Servs., No. 08-5805 (E.D. Pa. filed Dec. 16, 2008), <https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081216gatewaycmpt.pdf>; Complaint, FTC v. Golden Empire Mortgage, Inc., No. 09-03227 CAS(SHx) (C.D. Cal. filed May 7, 2009), <https://www.ftc.gov/sites/default/files/documents/cases/2009/05/090511gemcmpt.pdf>.

113 *See, e.g.*, Big Data Tr. 179–83 (Peter Swire), 187–90 (Peter Swire, Leonard Chanin, and C. Lee Peeler in conversation), 204–05 (Peter Swire), 268–69 (Christopher Calabrese).

114 In the context of mortgage advertising, creditors should also consider the FHA. 42 U.S.C. §§ 3601–3631; 24 C.F.R. Parts 100, 103, and 104. Regulations that implement the FHA prohibit “[f]ailing or refusing to provide to any person information regarding the availability of loans or other financial assistance, application requirements, procedures or standards for the review and approval of loans or financial assistance, or providing information which is inaccurate or different from that provided others, because of race, color, religion, sex, handicap, familial status, or national origin.” 24 C.F.R. § 100.120(b)(1).

115 15 U.S.C. § 1691(a)(1).

impact in subsequent lending.<sup>116</sup> Nevertheless, companies should proceed with caution in this area. In credit transactions,<sup>117</sup> Regulation B, which is the implementing regulation for ECOA, prohibits creditors<sup>118</sup> from making oral or written statements, in advertising or otherwise, to applicants or prospective applicants that would discourage on a prohibited basis a reasonable person from making or pursuing an application.<sup>119</sup> With respect to prescreened solicitations, Regulation B also requires creditors to maintain records of the solicitations and the criteria used to select potential recipients.<sup>120</sup> Advertising and marketing practices could impact a creditor's subsequent lending patterns and the terms and conditions of the credit received by borrowers, even if credit offers are open to all who apply. In some cases, the DOJ has cited a creditor's advertising choices as evidence of discrimination.<sup>121</sup>

Ultimately, as with the FCRA, the question of whether a practice is unlawful under equal opportunity laws is a case-specific inquiry. Accordingly, companies should proceed with caution if their practices could suggest disparate treatment or have a demonstrable disparate impact based on protected characteristics.

### 3. The Federal Trade Commission Act

Section 5 of the Federal Trade Commission Act ("Section 5") prohibits unfair or deceptive acts or practices in or affecting commerce.<sup>122</sup> Unlike the FCRA or equal opportunity laws, Section 5 is not confined to particular market sectors but is generally applicable to most companies acting in commerce.<sup>123</sup> Under Section 5, an act or practice is *deceptive* if it involves a material statement or omission that is likely to mislead a consumer acting reasonably under the circumstances.<sup>124</sup> For example, if a company violates a material promise—whether that

116 See, e.g., Big Data Tr. 178–191 (Peter Swire, C. Lee Peeler, and Leonard Chanin in conversation).

117 Under Regulation B, credit transaction means "every aspect of an applicant's dealings with a creditor regarding an application for credit or an existing extension of credit (including, but not limited to, information requirements; investigation procedures; standards of creditworthiness; terms of credit; furnishing of credit information; revocation, alteration, or termination of credit; and collection procedures)." 12 C.F.R. § 1002.2(m).

118 Under Regulation B, a creditor "does not include a person whose only participation in a credit transaction involves honoring a credit card." *Id.* § 1002.2(l).

119 *Id.* § 1002.4(b).

120 *Id.* § 1002.12(b)(7).

121 See, e.g., Complaint, United States v. First United Sec. Bank, No. 1 09-cv-00644 (S.D. Ala. filed Sept. 30, 2009), <http://www.justice.gov/sites/default/files/crt/legacy/2010/12/14/fuscomp.pdf>.

122 15 U.S.C. § 45(a)(1) (2012).

123 The FTC's consumer protection mandate is broad. Under Section 5 of the FTC Act, 15 U.S.C. § 45, the Commission has the power to prevent "persons, partnerships, and corporations" from using unfair or deceptive acts or practices in or affecting commerce, with certain limited exceptions. Those exceptions include: (1) banks and savings and loan institutions as described in 15 U.S.C. § 57a(f)(2) and (3); (2) federal credit unions as described in 15 U.S.C. § 57a(f)(4); (3) common carrier activities subject to subtitle IV of title 49 and the Communications Act of 1934; and (4) air carriers and foreign air carriers.

124 FTC Policy Statement on Deception, 103 F.T.C. 110, 174 (1984) (appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984)). See also POM Wonderful LLC, No. C-9344, 2013 WL 268926, at \*18 (F.T.C. Jan. 16, 2013).



promise is to refrain from sharing data with third parties,<sup>125</sup> to provide consumers choices about sharing,<sup>126</sup> or to safeguard consumers' personal information<sup>127</sup>—it will likely be engaged in a deceptive practice under Section 5.

Likewise, a failure to disclose material information may violate Section 5. In *CompuCredit*, for instance, the FTC included an allegation in the complaint that although a credit card marketing company touted the ability of consumers to use the card for cash advances, it deceptively failed to disclose that, based on a behavioral scoring model, consumers' credit lines would be reduced if they used their cards for such cash advances or if they used their cards for certain types of transactions, including marriage counseling, bars and nightclubs, pawn shops, and massage parlors.<sup>128</sup> Among other things, the settlement prohibits CompuCredit from making misrepresentations to consumers in the marketing of credit cards, including misrepresentations about the amount of available credit.<sup>129</sup>

In addition, under Section 5, an act or practice is *unfair* if it is likely to cause substantial consumer injury, the injury is not reasonably avoidable by consumers, and the injury is not outweighed by benefits to consumers or competition.<sup>130</sup> One example of a potentially unfair practice is the failure to reasonably secure consumers' data where that failure is likely to cause substantial injury.<sup>131</sup> Companies that maintain big data on consumers should take care to reasonably secure that data commensurate with the amount and sensitivity

125 See, e.g., Goldenshores Techs., LLC, No. C-4446 (F.T.C. Mar. 31, 2014), <https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf>; FTC v. Myspace LLC, No. C-4369 (F.T.C. Aug. 30, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacedo.pdf>.

126 See, e.g., Compete, Inc., No. D-4384 (F.T.C. Feb. 20, 2013), <https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competedo.pdf>; United States v. Path, Inc., No. C-13-0448 (N.D. Cal. Feb. 8, 2013), <https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf>; Google Inc., No. C-4336 (F.T.C. Oct. 13, 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf>; Facebook, Inc., No. C-4365 (F.T.C. July 27, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>; Chitika, Inc., No. C-4324 (F.T.C. June 7, 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikado.pdf>.

127 See, e.g., Snapchat, Inc., C-4501 (F.T.C. Dec. 23, 2014), <https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf>; Fandango, LLC, No. C-4481 (F.T.C. Aug. 13, 2014), <https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf>; Credit Karma, Inc., C-4480 (F.T.C. Aug. 13, 2014), <https://www.ftc.gov/system/files/documents/cases/1408creditkarmado.pdf>; Twitter, Inc., No. C-4316 (F.T.C. Mar. 2, 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf>; Reed Elsevier Inc., No. C-4226 (F.T.C. July 29, 2008), <https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reeddo.pdf>.

128 Complaint, *CompuCredit*, No. 1:08-cv-1976-BBM-RGV (N.D. Ga. filed June 10, 2008), <https://www.ftc.gov/sites/default/files/documents/cases/2008/06/080610compucreditcmplt.pdf>.

129 *Id.*

130 15 U.S.C. § 45(n) (2012). See also FTC Policy Statement on Unfairness (appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984)).

131 See, e.g., GMR Transcription Servs., Inc., No. C-4482 (F.T.C. Aug. 14, 2014), <https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf>; GeneWize Life Scis., Inc., No. C-4457 (F.T.C. May 8, 2014), <https://www.ftc.gov/system/files/documents/cases/140512foruintndo.pdf>; HTC Am., Inc., No. C-4406 (F.T.C. June 25, 2013), <https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf>; Compete, No. C-4384 (F.T.C. Feb. 20, 2013), <https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competedo.pdf>; Upromise, Inc., No. C-4351 (F.T.C. Mar. 27, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisedo.pdf>.

of the data at issue, the size and complexity of the company's operations, and the cost of available security measures.<sup>132</sup> For example, a company that maintains Social Security numbers or medical information about individual consumers should have particularly robust security measures as compared to a company that maintains consumers' names only.

Another example of a potentially unfair practice that the Commission has challenged is the sale of data to customers that a company knows or has reason to know will use the data for fraudulent purposes. The Commission's cases against Sequoia One and ChoicePoint are instructive in this regard. In *Sequoia One*, the FTC's complaint alleges that the company sold the personal information of financially distressed payday loan applicants—including Social Security numbers, financial account numbers, and bank routing numbers—to non-lender third-parties and one of these third parties used the information to withdraw millions of dollars from consumers' accounts without their authorization.<sup>133</sup>

In *ChoicePoint*, the Commission alleged that the company sold the personal information of more than 163,000 consumers to identity thieves posing as legitimate subscribers, despite obvious red flags that should have alerted the company to the potential fraud.<sup>134</sup> As these cases show, at a minimum, companies must not sell their big data analytics products to customers if they know or have reason to know that those customers will use the products for fraudulent purposes.

Section 5 may also apply under similar circumstances if products are sold to customers that use the products for discriminatory purposes.<sup>135</sup> The inquiry will be fact-specific, and in every case, the test will be whether the company is offering or using big data analytics in a deceptive or unfair way.

<sup>132</sup> See generally FED. TRADE COMM'N, *START WITH SECURITY: A GUIDE FOR BUSINESS* (2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

<sup>133</sup> FTC v. Sequoia One, LLC, No. 2:15-cv-01512 (D. Nev. Aug. 10, 2015), <https://www.ftc.gov/system/files/documents/cases/150812sequoiaonemcdonnellstip.pdf>; Complaint, *Sequoia One*, No. 2:15-cv-01512 (D. Nev. filed Aug. 7, 2015), <https://www.ftc.gov/system/files/documents/cases/150812sequoiaonecmpt.pdf>. See also Press Release, Fed. Trade Comm'n, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts (Dec. 23, 2014), <https://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars>. In *LeapLab*, the Commission's complaint alleges that the company bought payday loan applications of financially strapped consumers, and then sold that information—including Social Security numbers and financial account numbers—to marketers whom it knew had no legitimate need for it. Complaint at 5–10, LeapLab, LLC, No. 2:14-cv-02750 (D. Ariz. filed Dec. 22, 2014), <https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf>. One of these marketers allegedly used the information to withdraw millions of dollars from consumers' accounts without their authorization. *Id.* at 9–10.

<sup>134</sup> United States v. ChoicePoint, Inc., No. 1:06-cv-0198-JTC (N.D. Ga. Feb. 15, 2006), <https://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf>.

<sup>135</sup> Cf. DATA BROKERS REPORT, *supra* note 7, at 56.

### Questions for Legal Compliance

In light of these existing laws, companies already using or considering engaging in big data analytics should, among other things, consider the following:

- If you compile big data for others who will use it for eligibility decisions (such as credit, employment, insurance, housing, government benefits, and the like), are you complying with the accuracy and privacy provisions of the FCRA? FCRA requirements include requirements to (1) have reasonable procedures in place to ensure the maximum possible accuracy of the information you provide, (2) provide notices to users of your reports, (3) allow consumers to access information you have about them, and (4) allow consumers to correct inaccuracies.
- If you receive big data products from another entity that you will use for eligibility decisions, are you complying with the provisions applicable to users of consumer reports? For example, the FCRA requires that entities that use this information for employment purposes certify that they have a "permissible purpose" to obtain it, certify that they will not use it in a way that violates equal opportunity laws, provide pre-adverse action notice to consumers, and thereafter provide adverse action notices to those same consumers.
- If you are a creditor using big data analytics in a credit transaction, are you complying with the requirement to provide statements of specific reasons for adverse action under ECOA? Are you complying with ECOA requirements related to requests for information and record retention?
- If you use big data analytics in a way that might adversely affect people in their ability to obtain credit, housing, or employment:
  - Are you treating people differently based on a prohibited basis, such as race or national origin?
  - Do your policies, practices, or decisions have an adverse effect or impact on a member of a protected class, and if they do, are they justified by a legitimate business need that cannot reasonably be achieved by means that are less disparate in their impact?
- Are you honoring promises you make to consumers and providing consumers material information about your data practices?
- Are you maintaining reasonable security over consumer data?
- Are you undertaking reasonable measures to know the purposes for which your customers are using your data?
  - If you know that your customer will use your big data products to commit fraud, do not sell your products to that customer. If you have reason to believe that your data will be used to commit fraud, ask more specific questions about how your data will be used.
  - If you know that your customer will use your big data products for discriminatory purposes, do not sell your products to that customer. If you have reason to believe that your data will be used for discriminatory purposes, ask more specific questions about how your data will be used.

## B. Special Policy Considerations Raised by Big Data Research

Workshop and seminar panelists, academics, and others have also engaged in important research in the field of big data.<sup>136</sup> Some of this research has focused on how big data analytics could negatively affect low-income and underserved populations.<sup>137</sup> Researchers note there is a potential for incorporating errors and biases at every stage, from choosing the data set used to make predictions, to defining the problem to be addressed through big data, to making decisions based on the results of big data analysis.<sup>138</sup> While having the ability to use more data can increase the power of the analysis, simply adding more data does not necessarily correct inaccuracies or remove biases. In addition, the complexity of the data and statistical models can make it difficult for analysts to fully understand and explain the underlying model or its results. Even when data analysts are very careful, the results of their analysis may affect particular sets of individuals differently because their models may use variables that turn out to operate no differently than proxies for protected classes.<sup>139</sup> Or researchers may simply lack information that would allow them to determine whether their results have such effects. Numerous researchers and commenters discuss how big data could be used in the future to the disadvantage of low-income and underserved communities and adversely affect consumers on the basis of legally protected characteristics in hiring, housing, lending, and other processes.<sup>140</sup>

136 See generally Robinson + Yu Comment #00080, *supra* note 53; Ctr. for Data Innovation Comment #00055, *supra* note 8; Comment #00042 from Peter Swire, Ga. Inst. of Tech. & Future of Privacy Forum, to Fed. Trade Comm'n (Sept. 15, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/09/00042-92638.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/09/00042-92638.pdf); Future of Privacy Forum Comment #00027, *supra* note 23; Ctr. on Privacy & Tech. at Geo. L. Comment #00024, *supra* note 8; Nat'l Consumer L. Ctr. Comment #00018, *supra* note 1; N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8; World Privacy Forum Comment #00014, *supra* note 19; Tech. Pol'y Inst. Comment #00010, *supra* note 8; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8.

137 See, e.g., Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CAL. LAW R. \_ (forthcoming 2016), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2477899#](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899#); Alex Rosenblat et al., *Networked Employment Discrimination*, (Data & Society Research Inst., Working Paper Oct. 8, 2014), <http://www.datasociety.net/pubs/fow/EmploymentDiscrimination.pdf>; Gary Marcus & Ernest Davis, *Eight (No, Nine!) Problems With Big Data*, N.Y. TIMES (Apr. 6, 2014), [http://www.nytimes.com/2014/04/07/opinion/eight-no-nine-problems-with-big-data.html?\\_r=0](http://www.nytimes.com/2014/04/07/opinion/eight-no-nine-problems-with-big-data.html?_r=0); Tim Harford, *Big Data: Are We Making a Big Mistake?*, FT MAGAZINE (Mar. 28, 2014), <http://www.ft.com/intl/cms/s/2/21a6e7d8-b479-11e3-a09a-00144feabdc0.html>. See generally JOSEPH TUROW, THE DAILY YOU: HOW THE NEW ADVERTISING INDUSTRY IS DEFINING YOUR IDENTITY AND YOUR WORTH (2012).

138 See, e.g., Big Data Tr. 19–25 (Solon Barocas). See also Nat'l Consumer L. Ctr. Comment #00018, *supra* note 1, at 14–15; World Privacy Forum Comment #00014, *supra* note 19, at 6–17. See generally Barocas & Selbst, *supra* note 137.

139 Barocas & Selbst, *supra* note 137, at 20–22. Researchers note that data mining poses the additional problem of giving data miners the ability to disguise intentional discrimination as unintentional. *Id.* at 22–23. See also Paul Ohm, *Changing the Rules: General Principles for Data Use and Analysis*, in PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 100–02 (Julia Lane et al. eds., 2014). For examples of the kinds of analyses that can be conducted to detect whether model variables are proxies for protected characteristics, see generally FED. TRADE COMM'N, CREDIT-BASED INSURANCE SCORES: IMPACTS ON CONSUMERS OF AUTOMOBILE INSURANCE (2007), [http://www.ftc.gov/sites/default/files/documents/reports/credit-based-insurance-scores-impacts-consumers-automobile-insurance-report-congress-federal-trade/p044804facta\\_report\\_credit-based\\_insurance\\_scores.pdf](http://www.ftc.gov/sites/default/files/documents/reports/credit-based-insurance-scores-impacts-consumers-automobile-insurance-report-congress-federal-trade/p044804facta_report_credit-based_insurance_scores.pdf), and Bd. of Governors of the Fed. Reserve Sys., REPORT TO CONGRESS ON CREDIT SCORING AND ITS EFFECTS ON THE AVAILABILITY AND AFFORDABILITY OF CREDIT (2007), <http://www.federalreserve.gov/boarddocs/rptcongress/creditscore/creditscore.pdf>.

140 See generally Robinson + Yu Comment #00080, *supra* note 53; Am.'s Open Tech. Inst. Comment #00078, *supra* note 46; Ctr. for Democracy & Tech. Comment #00075, *supra* note 61; Am. Civil Liberties Union Comment #00059, *supra* note 61; Ctr. on Privacy & Tech. at Geo. L. Comment #00024, *supra* note 8; Nat'l Consumer L. Ctr. Comment #00018, *supra* note 1;

On the other hand, several stakeholders argue that these concerns are overstated.<sup>141</sup> Some emphasize that, to the extent the various steps in data mining lead to disparate impact, these issues are not new—they are inherent in any statistical analysis.<sup>142</sup> Other writers note that, rather than disadvantaging minorities in the hiring process, big data can help to create “a labor market that’s fairer to people at every stage of their careers.”<sup>143</sup> For example, companies can use big data algorithms to find employees from within underrepresented segments of the population.<sup>144</sup> They can also use big data to identify biases so that they can choose candidates based on merit rather than using mechanisms that depend on the reviewers’ biases.<sup>145</sup> Furthermore, as other stakeholders have noted, big data can help “reduce the rate of ‘false positive’ cases that potentially make disparate treatment a problem”<sup>146</sup> and can help identify whether correlations exist between prices and variables such as race, gender or ethnicity.<sup>147</sup> These stakeholders do not argue that we should ignore discrimination where it occurs; rather, they argue that we should recognize the potential benefits of big data to reduce discriminatory harm.

---

Common Sense Media Comment #00016, *supra* note 8; N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8; World Privacy Forum Comment #00014, *supra* note 19; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8. See also Barocas & Selbst, *supra* note 137; Crawford, *supra* note 39.

141 See, e.g., Big Data Tr. 75 (Gene Gsell). See generally Comment #00081 from Berin Szoka & Tom Struble, TechFreedom, & Geoffrey Manne & Ben Sperry, Int’l Ctr. for L. & Econ., to Fed. Trade Comm’n (Nov. 3, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/11/00081-92956.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/11/00081-92956.pdf); Comment #00074 from Howard Fienberg, Mktg. Research Assoc., to Fed. Trade Comm’n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00074-92927.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00074-92927.pdf); Comment #00070 from Bijan Madhani, Computer & Commc’ns Indus. Assoc., to Fed. Trade Comm’n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00070-92912.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00070-92912.pdf); NetChoice Comment #00066, *supra* note 23; Ctr. for Data Innovation Comment #00055, *supra* note 8; Ctr. for Data Innovation Comment #00026, *supra* note 8; Tech. Pol’y Inst. Comment #00010, *supra* note 8; VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK* (2013).

142 See, e.g., Dan Gray, *Ethics, Privacy and Discrimination in the Age of Big Data*, DATAECONOMY (Dec. 3, 2014), <http://dataconomy.com/ethics-privacy-and-discrimination-in-the-age-of-big-data/>. But see Jeff Leek, *Why Big Data Is in Trouble: They Forgot About Applied Statistics*, SIMPLYSTATS (May 7, 2014), <http://simplystatistics.org/2014/05/07/why-big-data-is-in-trouble-they-forgot-about-applied-statistics/> (noting that big data users have not given sufficient attention to issues that statisticians have been thinking about for a long time: sampling populations, multiple testing, bias, and overfitting).

143 See, e.g., Don Peck, *They’re Watching You at Work*, ATLANTIC (Dec. 2013), <http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/>.

144 See, e.g., Big Data Tr. 126 (Mark MacCarthy), 251 (Christopher Wolf). See also Software & Info. Indus. Assoc. Comment #00067, *supra* note 2, at 7; Future of Privacy Forum Comment #00027, *supra* note 23, attached report entitled, *BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS*, at 1–2.

145 See, e.g., Anne Loehr, *Big Data for HR: Can Predictive Analytics Help Decrease Discrimination in the Workplace?*, HUFFINGTON POST (Mar. 23, 2015), [http://www.huffingtonpost.com/anne-loehr/big-data-for-hr-can-predi\\_b\\_6905754.html](http://www.huffingtonpost.com/anne-loehr/big-data-for-hr-can-predi_b_6905754.html).

146 WHITE HOUSE FEB. 2015 REPORT, *supra* note 56, at 16.

147 *Id.* at 17. Economists have documented ways that data can help identify discrimination against protected groups in a wide variety of settings. For example, a randomized experiment changed the names on resumes sent to employers from white-sounding names to African-American sounding names; resumes with white-sounding names were 50 percent more likely to be called back for an interview. Marianne Bertrand & Sendhil Mullainathan, *Are Emily and Greg More Employable Than Lakisha and Jamal? A Field Experiment on Labor Market Discrimination*, 94 AM. ECON. REV. 991, 991–1013 (2004). Research from the early days of the Internet found that African-Americans and Latinos paid about 2 percent more for used cars purchased offline, but paid similar prices for those purchased online; the proffered reason was that individuals were anonymous online. Fiona Scott Morton et al., *Consumer Information and Discrimination: Does the Internet Affect the Pricing of New Cars to Women and Minorities?*, 1 QUANTITATIVE MKTG. & ECON. 65, 65–92 (2003). See also Devin Pope & Justin Sydnor, *Implementing Anti-Discrimination Policies in Statistical Profiling Models*, 3 AM. ECON. J.: ECON. POL’Y 206, 206–231 (2011), [http://faculty.chicagobooth.edu/devin.pope/research/pdf/Website\\_Antidiscrimination%20Models.pdf](http://faculty.chicagobooth.edu/devin.pope/research/pdf/Website_Antidiscrimination%20Models.pdf).

Collectively, this research suggests that big data offers both new potential discriminatory harms and new potential solutions to discriminatory harms. To maximize the benefits and limit the harms, companies should consider the questions raised by research in this area. These questions include the following:

### 1. How representative is your data set?

Workshop participants and researchers note that the data sets, on which all big data analysis relies, may be missing information about certain populations, e.g., individuals who are more careful about revealing information about themselves, who are less involved in the formal economy, who have unequal access or less fluency in technology resulting in a digital divide<sup>148</sup> or data desert,<sup>149</sup> or whose behaviors are simply not observed because they are believed to be less profitable constituencies.<sup>150</sup>

Recent examples demonstrate the impact of missing information about particular populations on data analytics. For example, Hurricane Sandy generated more than twenty million tweets between October 27 and November 1, 2012.<sup>151</sup> If organizations were to use this data to determine where services should be deployed, the people who needed services the most may not have received them. The greatest number of tweets about Hurricane Sandy came from Manhattan, creating the illusion that Manhattan was the hub of the disaster. Very few messages originated from more severely affected locations, such as Breezy Point, Coney Island, and Rockaway—areas with lower levels of smartphone ownership and Twitter usage. As extended power blackouts drained batteries and limited cellular access, even fewer tweets came from the worst hit areas. As one researcher noted, “data are assumed to accurately reflect the social world, but there are significant gaps, with little or no signal coming from particular communities.”<sup>152</sup>

Organizations have developed ways to overcome this issue. For example, the city of Boston developed an application called Street Bump that utilizes smartphone features such as GPS feeds to collect and report to the city information about road conditions, including potholes. However, after the release of the application, the Street Bump team recognized that because lower income individuals may be less likely to carry smartphones, the data was likely not fully representative of all road conditions. If the city had

148 A digital divide refers to the fact that certain populations may not have access to the Internet. See, e.g., Ctr. for Data Innovation Comment #00055, *supra* note 8, at 2; Nat'l Consumer L. Ctr. Comment #00018, *supra* note 1, at 9, 27; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8, at 2.

149 Data deserts are geographic “areas characterized by a lack of access to high-quality data that may be used to generate social and economic benefits.” Ctr. for Data Innovation, Comment #00055, *supra* note 8, at 3. “[I]f some communities are not represented in the data, decisions may overlook members of these communities and their unique needs.” *Id.*, attached report entitled, WIKIPEDIA EDITS REVEAL AMERICA'S DATA DESERTS, at 1.

150 See, e.g., Big Data Tr. 100–02 (Dr. Nicol Turner-Lee), 256–58 (Daniel Castro). See also Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8, at 2; Quentin Hardy, *Why Big Data Is Not Truth*, N.Y. TIMES (June 1, 2013), [http://bits.blogs.nytimes.com/2013/06/01/why-big-data-is-not-truth/?\\_php=true&\\_type=blogs&\\_r=1](http://bits.blogs.nytimes.com/2013/06/01/why-big-data-is-not-truth/?_php=true&_type=blogs&_r=1) (reviewing a speech provided by Kate Crawford); danah boyd & Kate Crawford, *Critical Questions for Big Data*, 15 INFO., COMM'N & Soc'y 662, 668–70 (2012), <http://dx.doi.org/10.1080/1369118X.2012.678878>.

151 See, e.g., Crawford, *supra* note 39. See also Grinberg et al., *supra* note 37.

152 Crawford, *supra* note 39.

continued relying on the biased data, it might have skewed road services to higher income neighborhoods. The team addressed this problem by issuing its application to city workers who service the whole city and supplementing the data with that from the public.<sup>153</sup> This example demonstrates why it is important to consider the digital divide and other issues of underrepresentation and overrepresentation in data inputs before launching a product or service in order to avoid skewed and potentially unfair ramifications.

## 2. Does your data model account for biases?

While large data sets can give insight into previously intractable challenges, hidden biases at both the collection and analytics stages of big data's life cycle could lead to disparate impact.<sup>154</sup> Researchers have noted that big data analytics "can reproduce existing patterns of discrimination, inherit the prejudice of prior decision-makers, or simply reflect the widespread biases that persist in society."<sup>155</sup> For example, if an employer uses big data analytics to synthesize information gathered on successful existing employees to define a "good employee candidate," the employer could risk incorporating previous discrimination in employment decisions into new employment decisions.<sup>156</sup> Even prior to the widespread use of big data, there is some evidence of the use of data leading to the reproduction of existing biases. For example, one researcher has noted that a hospital developed a computer model to help identify "good medical school applicants" based on performance levels of previous and existing students, but, in doing so, the model reproduced prejudices in prior admission decisions.<sup>157</sup>

Companies can also design big data algorithms that learn from human behavior; these algorithms may "learn" to generate biased results. For example, one academic found that Reuters and Google queries for names identified by researchers to be associated with African-Americans were more likely to return advertisements for arrest records than for names identified by researchers to be associated with white Americans.<sup>158</sup> The academic concluded that determining why this discrimination was occurring was beyond the scope of her research, but reasoned that search engines' algorithms may learn to prioritize arrest record ads for searches of names associated with African-Americans if people click on such ads more frequently than other ads.<sup>159</sup> This could reinforce the display of such ads and perpetuate the cycle.

153 See, e.g., Big Data Tr. 21–22 (Solon Barocas), 259–60 (Michael Spadea). See also Tech. Pol'y Inst. Comment #00010, *supra* note 8, at 4 & attached report at 15; WHITE HOUSE MAY 2014 REPORT, *supra* note 1, at 51–52.

154 See, e.g., Big Data Tr. 19–25 (Solon Barocas), 40–41 (Joseph Turow).

155 Barocas & Selbst, *supra* note 137, at 3–4.

156 See, e.g., Big Data Tr. 168–70 (Carol Miaskoff). Cf. Barocas & Selbst, *supra* note 137, at 9–11.

157 See generally Stella Lowry & Gordon Macpherson, *A Blot on the Profession*, 296 BRITISH MED. J., 657, 657–58 (1988), <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2545288/pdf/bmj00275-0003.pdf>.

158 See generally Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMM'NS OF THE ACM 44 (2013), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2208240&download=yes](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208240&download=yes). See also Big Data Tr. 64–65 (David Robinson); Robinson + Yu Comment #00080, *supra* note 53, at 16–17; N.Y.U. Info. L. Inst. Comment #00015, *supra* note 8, at 6.

159 Sweeney, *supra* note 158, at 34. See also Bianca Bosker, *Google's Online Ad Results Guilty of Racial Profiling, According to New Study*, HUFFINGTON POST (Feb. 5, 2013), <http://www.huffingtonpost.com/2013/02/05/online->

Companies should therefore think carefully about how the data sets and the algorithms they use have been generated. Indeed, if they identify potential biases in the creation of these data sets or the algorithms, companies should develop strategies to overcome them. As noted above, Google changed its interview and hiring process to ask more behavioral questions and to focus less on academic grades after discovering that replicating its existing definitions of a “good employee” was resulting in a homogeneous tech workforce.<sup>160</sup> More broadly, companies are starting to recognize that if their big data algorithms only consider applicants from “top tier” colleges to help them make hiring decisions, they may be incorporating previous biases in college admission decisions.<sup>161</sup> As in the examples discussed above, companies should develop ways to use big data to expand the pool of qualified applicants they will consider.<sup>162</sup>

### 3. How accurate are your predictions based on big data?

Some researchers have also found that big data analysis does not give sufficient attention to traditional applied statistics issues, thus leading to incorrect results and predictions.<sup>163</sup> They note that while big data is very good at detecting correlations, it does not explain which correlations are meaningful.<sup>164</sup>

A prime example that demonstrates the limitations of big data analytics is Google Flu Trends, a machine-learning algorithm for predicting the number of flu cases based on Google search terms. To predict the spread of influenza across the United States, the Google team analyzed the top fifty million search terms for indications that the flu had broken out in particular locations. While, at first, the algorithms appeared to create accurate predictions of where the flu was more prevalent, it generated highly inaccurate estimates over time.<sup>165</sup> This could be because the algorithm failed to take into account certain variables. For example, the algorithm may not have taken into account that people would be more likely to search for flu-related terms if the local news ran a story on a flu outbreak, even if the outbreak occurred halfway around the world. As one researcher has noted, Google Flu Trends demonstrates that a “theory-free analysis of mere correlations is inevitably fragile.

---

[racial-profiling\\_n\\_2622556.html](#) (“[O]ver time, as certain templates are clicked more frequently than others, Google will attempt to optimize its customer’s ad by more frequently showing the ad that garners the most clicks.”).

160 See *supra* notes 35–36 and accompanying text. See also Am.’s Open Tech. Inst. Comment #00078, *supra* note 46, at 60–61.

161 Cf. Matt Richtel, *How Big Data Is Playing Recruiter for Specialized Workers*, N.Y. TIMES (Apr. 27, 2013), <http://www.nytimes.com/2013/04/28/technology/how-big-data-is-playing-recruiter-for-specialized-workers.html> (noting that some companies are using technology to find candidates based on their ability to succeed on the job rather than traditional markers, such as a degree from a top college).

162 The Commission recognizes that, to address data sets that incorporate previous prejudices, companies may need to collect demographic information about consumers that they would not otherwise collect. If they do collect this information, they should provide disclosures and choices to consumers where appropriate.

163 See, e.g., David Lazer et al., *The Parable of Google Flu: Traps in Big Data Analysis*, 343 SCI. 1203, 1203–05 (2014), <http://gking.harvard.edu/files/gking/files/0314policyforumff.pdf>; Marcus & Davis, *supra* note 137; Steve Lohr, *Google Flu Trends: The Limits of Big Data*, N.Y. TIMES (Mar. 28, 2014), [http://bits.blogs.nytimes.com/2014/03/28/google-flu-trends-the-limits-of-big-data/?\\_r=0](http://bits.blogs.nytimes.com/2014/03/28/google-flu-trends-the-limits-of-big-data/?_r=0).

164 See, e.g., Marcus & Davis, *supra* note 137. Likewise, these researchers note that whenever the source of information for a big data analysis is itself a product of big data, opportunities for reinforcing errors exist. See *id.*

165 See *supra* note 163 and accompanying text. Cf. Tech. Pol’y Inst. Comment #00010, *supra* note 8, attached report at 5–6.



If you have no idea what is behind a correlation, you have no idea what might cause that correlation to break down.”<sup>166</sup>

As another example, workshop participants discussed the fact that lenders can improve access to credit by using non-traditional indicators, e.g., rental or utility bill payment history.<sup>167</sup> Consumers, however, have the right to withhold rent if their landlord does not provide heat or basic sanitation services. In these instances, simply compiling rental payment history would not necessarily demonstrate whether the person is a good credit risk.<sup>168</sup>

In some cases, these sources of inaccuracies are unlikely to have significant negative effects on consumers. For example, it may be that big data analytics shows that 30 percent of consumers who buy diapers will respond to an ad for baby formula. That response rate may be enough for a marketer to find it worthwhile to send buyers of diapers an advertisement for baby formula. The 70 percent of consumers who buy diapers but are not interested in formula can disregard the ad or discard it at little cost. Similarly, consumers who are interested in formula and who do not buy diapers are unlikely to be substantially harmed because they did not get the ad.

On the other hand, if big data analytics are used as the basis for access to credit, housing, or other similar benefits, the potential effects on consumers from inaccuracies could be substantial.<sup>169</sup> For example, suppose big data analytics predict that people who do not participate in social media are 30 percent more likely to be identity thieves, leading a fraud detection tool to flag such people as “risky.” Suppose further that a wireless company uses this tool and requires “risky” people to submit additional documentation before they can obtain a cell phone contract. These people may not be able to obtain the contract if they do not have the required documentation. And they may never know why they were denied the ability to complete

166 Harford, *supra* note 137, at 133.

167 See, e.g., Big Data Tr. 51–52 (David Robinson), 83–84 (Mark MacCarthy), 102–06 (Stuart Pratt), 231–32 (Michael Spadea). See also Software & Info. Indus. Assoc. Comment #00067, *supra* note 2, at 5–6 and attached report at 7; Tech. Pol’y Inst. Comment #00010, *supra* note 8, at 5–6.

168 Some workshop participants and commenters note other challenges of using utility payments as a non-traditional indicator. See, e.g., Big Data Tr. 51–53 (David Robinson). See also Robinson + Yu Comment #00080, *supra* note 53, at 10–11; Nat’l Consumer L. Ctr. Comment #00018, *supra* note 1, at 13–14; Ctr. for Dig. Democracy & U.S. PIRG Educ. Fund Comment #00003, *supra* note 8, at 17.

169 See, e.g., Frank Pasquale, *The Dark Market for Personal Data*, N.Y. TIMES (Oct. 16, 2014), <http://mathbabe.org/2014/06/25/the-dark-matter-of-big-data/>; Boyd & Crawford, *supra* note 150, at 670–73; Ylan Q. Mui, Little Known Firms Tracking Data Used in Credit Scores, WASH. POST (July 16, 2011), [http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gtQAXHcWIL\\_story.html](http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gtQAXHcWIL_story.html). For the reasons set forth in her separate statement, Commissioner Ohlhausen believes that to assess properly any risks of harm from big data inaccuracies, such risks must be evaluated in the context of the competitive process.

the transaction or be able to correct the information used to flag them as “risky” even if the underlying information was inaccurate.<sup>170</sup>

In using big data to make decisions that affect consumers’ ability to complete transactions, companies should consider the potential benefits and harms, especially where their policies could negatively affect certain populations.

#### 4. Does your reliance on big data raise ethical or fairness concerns?

Companies should consider performing their own assessment of the factors that go into an analytics model and balancing the predictive value of the model with fairness considerations.<sup>171</sup> Indeed, overreliance on the predictions of big data analytics could potentially result in a company not thinking critically about the value, fairness, and other implications of their uses of big data.<sup>172</sup> For example, one company determined that employees who live closer to their jobs stay at these jobs longer than those who live farther away.<sup>173</sup> However, another company decided to exclude this factor from its hiring algorithm because of concerns about racial discrimination, particularly since different neighborhoods can have different racial compositions.<sup>174</sup>

Many companies are not only considering ethical concerns with using big data, but are actively using big data to advance the interests of minorities and fight discrimination. For example, there are now recruiting tools available that match companies in search of employees with candidates who hold the necessary qualifications, but also ensure that those candidates are not limited to particular gender, racial, and experiential backgrounds.<sup>175</sup> Individual companies are also changing their hiring techniques to promote

<sup>170</sup> See DATA BROKERS REPORT, *supra* note 7, at 53–54.

<sup>171</sup> See, e.g., Big Data Tr. 238–40 (Jeanette Fitzgerald). See generally The Internet Assoc. Comment #00073, *supra* note 23; Comment #00071 from Pam Dixon, World Privacy Forum, to Fed. Trade Comm’n (Oct. 31, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00071-92911.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00071-92911.pdf); Computer & Comm’n Indus. Assoc. Comment #00070, *supra* note 141; Consumer Elecs. Assoc. Comment #00068, *supra* note 61; Intel Corp. Comment #00062, *supra* note 61; Comment #00060 from Yael Weinman, Info. Tech. Indus. Council, to Fed. Trade Comm’n (Oct. 27, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00060-92877.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00060-92877.pdf); Info. Accountability Found. Comment #00049, *supra* note 2; Comment #00048 from Bojana Bellamy & Markus Heyder, Ctr. for Info. Pol’y Leadership, to Fed. Trade Comm’n (Oct. 8, 2014), [https://www.ftc.gov/system/files/documents/public\\_comments/2014/10/00048-92775.pdf](https://www.ftc.gov/system/files/documents/public_comments/2014/10/00048-92775.pdf); Future of Privacy Forum Comment #00027, *supra* note 23.

<sup>172</sup> See, e.g., Michael Schrage, *Big Data’s Dangerous New Era of Discrimination*, HARV. BUS. REV. (Jan. 29, 2014), <https://hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination/>. Cf. Alessandro Acquisti et al., *Face Recognition and Privacy in the Age of Augmented Reality*, 6 J. OF PRIVACY & CONFIDENTIALITY 1–20 (2014), <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1122&context=jpc> (showing that big data analytics can now identify strangers online (on a dating site where individuals protect their identities by using pseudonyms) and offline (in a public space), based on photos made publicly available on a social network site, and then infer additional and sensitive information about those consumers with relative ease).

<sup>173</sup> See, e.g., Robinson + Yu Comment #00080, *supra* note 53, at 15. See also Joseph Walker, *Meet The New Boss: Big Data*, WALL ST. J. (Sept. 20, 2012), <http://online.wsj.com/news/articles/SB10000872396390443890304578006252019616768>.

<sup>174</sup> See *supra* note 173.

<sup>175</sup> See, e.g., Future of Privacy Forum Comment #00027, *supra* note 23, attached report entitled, BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS, at 1.

diversity.<sup>176</sup> Xerox now uses an online evaluation tool developed by a data analytics firm to assess applicants, in addition to conducting interviews, to determine which applicants are most qualified for available jobs.<sup>177</sup> In developing this new assessment process, Xerox also learned that previous similar employment experience—one of the few criteria that Xerox had explicitly prioritized in the past—turns out to have no bearing on either productivity or retention.<sup>178</sup>

In addition, state and local government entities are using big data to help underrepresented communities obtain better municipal services. For example, states are using big data to identify the needs of lesbian, gay, bisexual, and transgender individuals and to create more tailored approaches to reduce health disparities impacting these individuals.<sup>179</sup> And big data was used to convince a city to redraw its boundaries to extend city services to historically African-American neighborhoods.<sup>180</sup> As these examples show, organizations can use big data in ways that provide opportunity to underrepresented and underserved communities.

### Summary of Research Considerations

In light of this research, companies already using or considering engaging in big data analytics should:

- Consider whether your data sets are missing information from particular populations and, if they are, take appropriate steps to address this problem.
- Review your data sets and algorithms to ensure that hidden biases are not having an unintended impact on certain populations.
- Remember that just because big data found a correlation, it does not necessarily mean that the correlation is meaningful. As such, you should balance the risks of using those results, especially where your policies could negatively affect certain populations. It may be worthwhile to have human oversight of data and algorithms when big data tools are used to make important decisions, such as those implicating health, credit, and employment.
- Consider whether fairness and ethical considerations advise against using big data in certain circumstances. Consider further whether you can use big data in ways that advance opportunities for previously underrepresented populations.

176 See, e.g., Tim Smedley, *Forget the CV, Data Decide Careers*, FIN. TIMES (July 9, 2014), <http://www.ft.com/cms/s/2/e3561cd0-dd11-11e3-8546-00144feabdc0.html#axzz373wnep7>.

177 See, e.g., Peck, *supra* note 143.

178 *Id.*

179 See, e.g., Future of Privacy Forum Comment #00027, *supra* note 23, attached report entitled, BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS, at 4; Computer & Comm'ns Indus. Assoc. Comment #00070, *supra* note 141, at 6–7. See also Laura Nahmias, *State Agencies Launch LGBT Data-Collection Effort*, POLITICO N.Y. (July 24, 2014), <http://www.capitalnewyork.com/article/albany/2014/07/8549536/state-agencies-launch-lgbt-data-collection-effort>.

180 See, e.g., Future of Privacy Forum Comment #00027, *supra* note 23, attached report entitled, BIG DATA: A TOOL FOR FIGHTING DISCRIMINATION AND EMPOWERING GROUPS, at 3.

## V. Conclusion

Big data will continue to grow in importance, and it is undoubtedly improving the lives of underserved communities in areas such as education, health, local and state services, and employment. Our collective challenge is to make sure that big data analytics continue to provide benefits and opportunities to consumers while adhering to core consumer protection values and principles. For its part, the Commission will continue to monitor areas where big data practices could violate existing laws, including the FTC Act, the FCRA, and ECOA, and will bring enforcement actions where appropriate. In addition, the Commission will continue to examine and raise awareness about big data practices that could have a detrimental impact on low-income and underserved populations and promote the use of big data that has a positive impact on such populations. Given that big data analytics can have big consequences, it is imperative that we work together—government, academics, consumer advocates, and industry—to help ensure that we maximize big data's capacity for good while identifying and minimizing the risks it presents.



## Appendix: Separate Statement of Commissioner Maureen K. Ohlhausen

### Big Data: A Tool for Inclusion or Exclusion?

January 6, 2016

I support today's report on big data as a useful contribution to the ongoing policy discussion about the effect of big data analysis on low-income, disadvantaged, and vulnerable consumers. One part of the report summarizes the concerns of several privacy advocates and academics over the potential inaccuracies of big data analytics. I write separately to emphasize the importance of evaluating these opinions in the context of market and competitive forces that affect all companies using big data analytics.

The report details the use of big data as it affects low-income, disadvantaged, or vulnerable consumers. Importantly, the report describes some of the many ways companies are already using big data to benefit such consumers—and others. The report also recognizes big data's massive potential benefits. In addition, the report sketches the legal landscape implicated by big data and offers questions that companies may find useful as they apply big data techniques to solve their business challenges.

The report also describes certain concerns about big data tools raised by some consumer advocates and researchers. Specifically, some fear that big data analysis will produce inaccurate or incomplete results, and that actions based on such flawed analysis will harm low-income, disadvantaged, or vulnerable consumers.<sup>1</sup> For example, some worry that companies may use inaccurate big data analysis to deny opportunities to otherwise eligible low-income or disadvantaged consumers, or to fail to advertise high-quality lending products to eligible low-income customers.<sup>2</sup>

Concerns about the effects of inaccurate data are certainly legitimate, but policymakers must evaluate such concerns in the larger context of the market and economic forces companies face. Businesses have strong incentives to seek accurate information about consumers, whatever the tool. Indeed, businesses use big data specifically to increase accuracy. Our competition expertise tells us that if one company draws incorrect conclusions and misses opportunities, competitors with better analysis will strive to fill the gap.<sup>3</sup>

1 FED. TRADE COMM'N, *BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES* 8–11, 25–27 (2016). The report also references other concerns that big data analysis will be *too* accurate: companies will understand their consumers too well and misuse that data to the consumer's detriment. Market forces also constrain many such potential harms, but other such harms could actually undermine market forces. For example, the report describes concerns that unscrupulous businesses will use big data techniques to develop "sucker lists" of consumers particularly vulnerable to scams and misleading offers. The report does a good job laying out the existing legal framework that applies to such harmful uses.

2 *Id.* at 9–11.

3 A real world example of the competitive advantages of novel but accurate application of data analytics was famously chronicled in the book (and movie) *Moneyball*. See MICHAEL LEWIS, *MONEYBALL: THE ART OF WINNING AN UNFAIR GAME* (2004). Oakland's strategy succeeded precisely because it "liberated" baseball players from "unthinking prejudice rooted in baseball's traditions . . . allowing them to demonstrate their true worth." *Id.* at iv. Each baseball franchise continually faces

Therefore, to the extent that companies today misunderstand members of low-income, disadvantaged, or vulnerable populations, big data analytics combined with a competitive market may well *resolve* these misunderstandings rather than *perpetuate* them.<sup>4</sup> In particular, a company's failure to communicate premium offers to eligible consumers presents a prime business opportunity for a competitor with a better algorithm.<sup>5</sup>

To understand the benefits and risks of tools like big data analytics, we must also consider the powerful forces of economics and free-market competition. If we give undue credence to hypothetical harms, we risk distracting ourselves from genuine harms and discouraging the development of the very tools that promise new benefits to low income, disadvantaged, and vulnerable individuals.

Today's report enriches the conversation about big data. My hope is that future participants in this conversation will test hypothetical harms with economic reasoning and empirical evidence.<sup>6</sup>

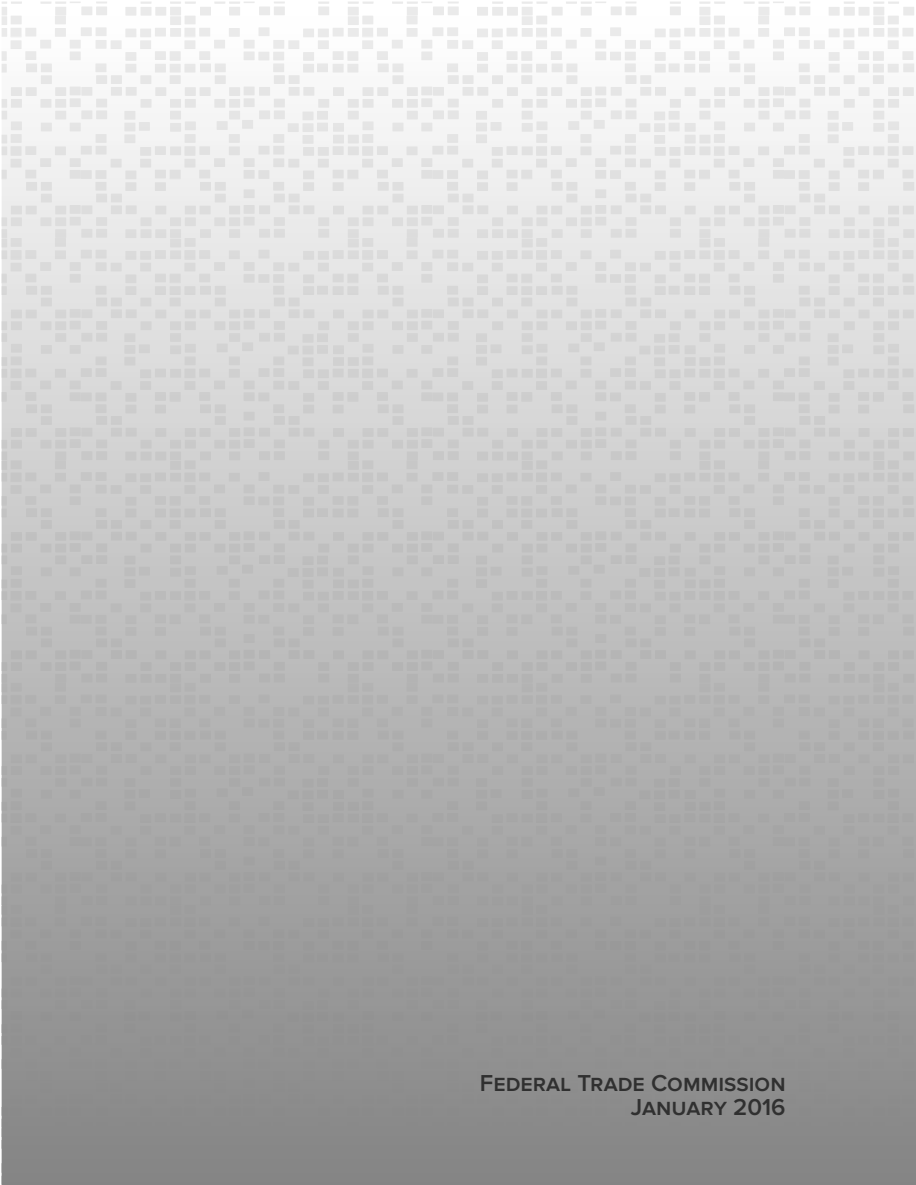
---

marketplace pressures to improve player quality predictions. Similarly, companies using big data analytics face competitive forces that punish inaccuracy and reward accuracy.

- 4 Indeed, there is strong theoretical and empirical economic evidence that low income and other disadvantaged households stand to gain more than the wealthy from many applications of big data analytics. See JAMES C. COOPER, SEPARATION, POOLING, AND PREDICTIVE PRIVACY HARMS FROM BIG DATA: CONFUSING BENEFITS FOR COSTS 38–49 (2015), <http://ssrn.com/abstract=2655794> (describing theoretical and empirical studies on the effects of big data in credit markets, price discrimination, and labor markets for low income individuals). One simple example: lenders do not need big data analytics to identify creditworthy high-income persons, as nearly all have credit files and most are lower-risk. However, lower-income groups contain both high- and low-risk borrowers. Big data analysis can help bring credit to the lower-risk low income borrowers with thin or no credit files. See *id.* at 38–39.
- 5 Transcript of Big Data: A Tool for Inclusion or Exclusion?, in Washington, D.C. (Sept. 15, 2014), at 231–32 (Daniel Castro and Michael Spaeda in conversation), [https://www.ftc.gov/system/files/documents/public\\_events/313371/bigdata-transcript-9\\_15\\_14.pdf](https://www.ftc.gov/system/files/documents/public_events/313371/bigdata-transcript-9_15_14.pdf) (highlighting the business opportunities in improved accuracy of credit scoring for low-income individuals). Indeed, our workshop on lead generation showed that lenders and other businesses are highly motivated to reach potential customers and spend a lot of money and effort to do so. See *generally Follow the Lead: An FTC Workshop on Lead Generation*, FED. TRADE COMM'N (Oct. 30, 2015), <https://www.ftc.gov/news-events/events-calendar/2015/10/follow-lead-ftc-workshop-lead-generation>.
- 6 For example, Cooper describes a useful framework to help identify under which conditions the presumption should be for or against big data uses. See COOPER, *supra* note 4, at 33–38.







FEDERAL TRADE COMMISSION  
JANUARY 2016

## NOTES

## NOTES

Article 29 Data Protection Working Party,  
European Commission, Statement on  
Statement of the WP29 on the impact of  
the development of big data on the protection  
of individuals with regard to the processing of  
their personal data in the EU  
(September 16, 2014)

Submitted by:  
Noga Rosenthal  
*Epsilon/Conversant*

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.





14/EN  
WP 221

**Statement on Statement of the WP29 on the impact of the development of  
big data on the protection of individuals with regard to the processing of  
their personal data in the EU**

**Adopted on 16 September 2014**

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 02/013.

Website: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)



The data protection authorities of the European Union, represented in the Article 29 Working Party (WP29), consider that the development of big data technologies can have important consequences on the protection of individuals with regard to the processing of their personal data in the EU.

The Working Party will continue to follow the development of this trend closely. For now, it has decided to publish the following statement to communicate a number of key messages on this issue.

\*\*\*\*

- Many individual and collective benefits are expected from the development of big data, despite the fact that the real value of big data still remains to be proven. The Working Party would naturally support genuine efforts at EU or national levels which aim to make these benefits real for individuals in the EU, whether individually or collectively.
- As an important part of big data operations relies on the extensive processing of the personal data of individuals in the EU, it also raises important social, legal and ethical questions, among which concerns with regard to the privacy and data protection rights of these individuals. The benefits to be derived from big data analysis can therefore be reached only under the condition that the corresponding privacy expectations of users are appropriately met and their data protection rights are respected.
- The EU legal framework for data protection is applicable to the processing of personal data in big data operations. Directive 95/46/EC and other relevant EU legal instruments are part of this framework. They ensure a high level of protection of individuals, namely by providing them with specific rights which cannot be waived.
- Some stakeholders assert that the application of some data protection principles and obligations under EU law should be substantially reviewed to enable promising forthcoming developments in big data operations to take place. The application of the principles of purpose limitation and data minimisation are presented as core concerns in this respect, as they require that data controllers collect personal data only for specified, explicit and legitimate purposes, and do not further process such data in a way incompatible with those purposes. They also require that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. In this regard, some voices argue that the focus should be only on the use of personal data, linking this to the level of risk of harm to individuals.
- The Working Party acknowledges that the challenges of big data might require innovative thinking on how some of these and other key data protection principles are applied in practice. However, at this stage, it has no reason to believe that the EU data protection principles, as they are currently enshrined in Directive 95/46/EC, are no longer valid and appropriate for the development of big data, subject to further improvements to make them more effective in practice. It also needs to be clear that the rules and principles are applicable to all processing operations, starting with collection in order to ensure a high level of data protection.
- In fact, the Working Party strongly believes that complying with this framework is a key element in creating and keeping the trust which any stakeholder needs in order to develop a stable business model that is based on the processing of such data. It also believes that compliance with this framework and investment in privacy-friendly solutions is essential to ensure fair and effective competition between economic players on the relevant markets. In



particular, upholding the purpose limitation principle is essential to ensure that companies which have built monopolies or dominant positions before the development of big data technologies hold no undue advantage over newcomers to these markets.

- "Big data" is a broad term that covers a great number of data processing operations, some of which are already well-identified, while others are still unclear and many more are expected to be developed in the near future.

- In addition, big data processing operations do not always involve personal data. Nevertheless, the retention and analysis of huge amounts of personal data in big data environments require particular attention and care. Patterns relating to specific individuals may be identified, also by means of the increased availability of computer processing power and data mining capabilities.

- A number of developments that are qualified today as big data – such as the development of comprehensive information systems in the delivery of health services or in the centralisation of law enforcement files, as well as behavioural advertising – have long been implemented in many EU Member States. These have already been addressed within the framework of the existing data protection rules, whether at EU or national levels.

- On the basis of these shared experiences, the Working Party recently released a number of policy documents which are relevant to the analysis of privacy concerns raised with regard to big data – e.g. Opinion 03/2013 on Purpose limitation, Opinion 05/2014 on Anonymisation techniques, Opinion 6/2014 on Legitimate interests or Opinion 01/2014 on the Application of necessity and proportionality concepts and data protection within the law enforcement sector.

- When necessary, the Working Party will initiate international cooperation with other relevant regulators in order to ensure the EU data protection rules are best applied in respect of the development of big data.

- The Working Party is further aware that international competition on big data means that different national, regional and international regulatory data protection and privacy frameworks may apply simultaneously at global level, which can entail important challenges in terms of compliance. In this light, the Working Party believes that increased cooperation is needed between data protection authorities and other competent authorities around the world on these issues. This cooperation is necessary to provide unified guidance and operational answers on the implementation of data protection rules to global players, as well as to implement joint enforcement of these rules, wherever possible. It is also necessary to reassure individuals that the protection of their data protection rights and interests is considered as fundamental by all stakeholders.

- Promoting cooperation between international regulators on big data needs to be firmly based on the different applicable legal frameworks. In Europe, the rights granted to the data subject by EU law (including transparency, rights of access, rectification, erasure, objection, right to be forgotten) result from a fundamental right. They are therefore generally applicable and only subject to limited exceptions provided by law.

## NOTES

## NOTES

16

Manatt, Phelps & Phillips, LLP, Advertising  
Law Newsletter (January–November 2016)

Submitted by:

Marc S. Roth

*Manatt, Phelps & Phillips, LLP*

© Manatt, Phelps & Phillips, LLP

If you find this article helpful, you can learn more about the subject by going to [www.pli.edu](http://www.pli.edu) to view the on demand program or segment for which it was written.



## Native Advertising

KEN BONE: BREAKOUT STAR, VIOLATOR OF FTC GUIDES? .....	2
YOUTUBE ADDS SPONSORED CONTENT NOTIFICATION FEATURE .....	2
CARU: SPONSORED VIDEOS NEED CLEAR, PROMINENT AUDIO DISCLOSURES .....	3
KARDASHIANS ACCUSED OF FAILING TO KEEP UP WITH FTC REGULATIONS .....	5
NAD RECOMMENDS GOOP LIFESTYLE BLOG CLEAN UP ITS CLAIMS .....	6
CONSUMER GROUPS URGE FTC ACTION ON INFLUENCERS .....	7
STUDY FINDS LOW COMPLIANCE FOR NATIVE ADVERTISING .....	8
SPECIAL FOCUS: LORD & TAYLOR SETTLES WITH FTC FOR NOT DISCLOSING NATIVE ADS .....	9
FTC'S BRILL TO ADVERTISERS: ENHANCE CONSUMER NOTICE, CONTROL .....	11
SPECIAL FOCUS: FTC ISSUES LONG-AWAITED NATIVE ADVERTISING GUIDANCE .....	13

## Social Media

PIN THIS: NEW CONTEST, SWEEPSTAKES RULES FOR PINTEREST .....	16
U.S. OLYMPIC COMMITTEE SUED OVER SOCIAL MEDIA OLYMPIC RULES .....	16
TWITTER SEEKS NINTH CIRCUIT RULING THAT IT DOES NOT "MAKE" CALLS .....	18
FIRST CIRCUIT AFFIRMS RULING AGAINST <a href="http://JERK.COM">JERK.COM</a> .....	20

## Mobile Marketing

NINTH CIRCUIT: CONFIRMATION TEXT MESSAGE DOESN'T VIOLATE TCPA .....	22
SPECIAL FOCUS: RESPONSES TO RETAIL WEBINAR ATTENDEE QUESTIONS .....	23
SPOKEO, INC. V. ROBINS: WHAT DOES IT MEAN FOR TCPA LAWSUITS? .....	25
PRIOR EXPRESS CONSENT EXISTS WHEN CELLPHONE NUMBER IS SHARED WITH INTERMEDIARY .....	27
LIMITED VOIP PLAN = CELLPHONE FOR TCPA PURPOSES, NEW YORK COURT RULES .....	30
TECH COMPANY SETTLES WITH FTC OVER INSTALLATION OF APPS WITHOUT PERMISSION .....	31
FCC CONFIRMS DIFFERENT TCPA LIABILITY ANALYSIS FOR TEXT, FAX BROADCASTERS .....	33
NINTH CIRCUIT AFFIRMS TCPA DISMISSAL BASED ON EXPRESS CONSENT .....	34
COURT CERTIFIES CLASS AGAINST YAHOO! FOR WELCOME MESSAGE .....	35



## Native Advertising

### Ken Bone: Breakout Star, Violator of FTC Guides?

November 04, 2016

**One thing folks on both sides of the political aisle can agree upon is that Ken Bone left the second presidential debate as a breakout star. But he may have tripped up when attempting to capitalize on his fame by sending a promotional tweet for Uber.**

Bone and his red sweater made just as many headlines as the candidates after he appeared as one of the undecided voters on the stage at the second debate and asked about energy policy.

In the days that followed, Bone rode the wave of his new fame with talk show appearances and a plug for car service Uber. As part of the company's launch of a black car service in St. Louis, Bone tweeted: "Everyone wants to know if I've decided ... and I have. uberSELECT helps you ride in style like me." Those who followed a link and entered promo code "KENBONE" received \$20 off their ride.

However, Bone failed to indicate that his tweet was sponsored, as required by the Federal Trade Commission's Endorsement Guides. While the Guides don't mandate the specific wording of disclosures, the agency recommends using words such as "advertising" or "promotion," and when facing character limits on social media platforms such as Twitter, "#ad."

When contacted about the problem, Uber indicated that the company provided Bone with Uber credit for his role in the launch. Bone did not respond when asked for a comment about the issue, but later deleted his promotional tweet and sent a new one apologizing: "#ad didn't know I had to do that. Sorry folks."

**Why it matters:** Uber certainly got publicity by making a connection with Bone, who said he had seven Twitter followers before the debate (two of whom were his grandmothers) and more than 200,000 afterwards. Whether Bone will remain a public figure remains to be seen, but at least he's aware of the requirements of the FTC Guides if he gets another endorsement opportunity.

### YouTube Adds Sponsored Content Notification Feature

October 20, 2016

To help influencers achieve compliance with the necessary disclosures about their relationships with advertisers, YouTube has unveiled a new tool to provide notice to viewers about sponsored content.

The new feature adds visible text on a video for the first few seconds watched by a viewer with a label stating "Includes paid promotion." Creators also have the ability to add the text to any existing videos without impacting their video metrics (such as view count).



"YouTube creators are among the most influential voices in media today," according to a post on the site's Creator Blog. "Since brands increasingly recognize the value of the connection creators have with their fans around the world, they are investing in collaborations to reach viewers in interesting and authentic ways. At the same time, viewers appreciate transparency when brands and creators collaborate on paid promotions such as product placements, sponsorships or endorsements."

The company also asked creators to check the "video contains paid promotion" box in their Video Managers, so that the site knows when a video contains removable sponsored content from the YouTube Kids app to comply with company policy.

YouTube cautioned creators that while the new feature is a helpful addition, different countries have their own sets of rules about how and when disclosures are required. Accordingly, "creators and brands should check and follow applicable laws as they may vary greatly," and provide links to regulators including the Federal Trade Commission and the Committee of Advertising Practice in the United Kingdom.

To read YouTube's blog post announcing the new tool, click [here](#).

**Why it matters:** The feature will be a helpful addition for influencers and other creators seeking to comply with disclosure requirements for sponsored content. Regulators have been increasingly cracking down on the failure to comply with disclosure requirements, as evidenced in recent actions by the Children's Advertising Review Unit and the Federal Trade Commission. The creative community should remember that simply using the notice provided by YouTube alone might not be sufficient to satisfy legal requirements, however.

## CARU: Sponsored Videos Need Clear, Prominent Audio Disclosures

September 29, 2016

**Taking a stand on social media influencers and the "unboxing" video trend, the Children's Advertising Review Unit (CARU) recommended that popular YouTube channels starring a ten-year-old and his family add a prominent audio disclosure before each new sponsored video.**

Evan and his family members (including younger sister Jillian and occasionally his parents) star in videos on three YouTube channels: EvanTubeHD, EvanTubeRAW, and EvanTubeGaming. The videos feature the family doing various activities of interest to children such as playing video games, performing science experiments, and unboxing toys. Evan's channels have millions of subscribers.

CARU expressed concern about these new media platforms, which "have heightened the possibility for confusion between advertising and editorial content, especially when it is viewed by children." Particularly problematic are "ostensibly user-generated online videos, which contain undisclosed or inadequately disclosed advertising or endorsements in the content of the videos themselves."

Roughly 85 percent of the videos posted on the Evan channels are made without any consideration from the manufacturers, the family told the self-regulatory body, and about 85 percent of the total revenue

generated by the channels comes from pre-roll advertising. When Evan does make a video featuring a free product or payment, he will sometimes make statements such as “When we came home from school we found a surprise from [Company],” or state that the video was “brought to you by [brand],” or use a text disclosure, e.g., “sponsored by [Company]” below the video.

CARU, however, determined that the sponsored videos amount not only to paid commercial advertising whose purpose is to induce the sale of a product and/or persuade the audience of the value of a product or brand, they are a form of native advertising.

But were those facts clear to the children watching the videos?

Not necessarily, CARU said, as “children would reasonably assume that all Channel posts, including sponsored ones, were independent unless there was a clear disclosure indicating otherwise” and the existing attempts at disclosure were insufficient.

Evan’s use of a text disclosure was not helpful for young children who do not know how to read, his comments in sponsored videos did not make clear that the products had been paid for, and the pre-roll ads at the beginning of the videos added to the confusion. “Because children may easily recognize these commercials as ads they may be even less likely to suspect that further advertisements are contained within the videos,” the self-regulatory body wrote.

CARU was also not persuaded that the use of phrases such as “brought to you by [brand]” or “sponsored by [brand]” were sufficient to put children on notice that they were viewing an ad.

“EvanTube should modify and standardize the way it provides disclosures,” CARU recommended. Disclosures on the channels should be enhanced in accordance with Federal Trade Commission guidance and CARU’s own guidelines in order to adequately inform children that the sponsored videos are advertisements.

“An effective disclosure informing consumers of the sponsored video’s commercial nature at the start is necessary to prevent consumer deception,” CARU said, adding that the channels should “place a clear and prominent audio disclosure stating that the videos are advertisements at the outset of the video before any such sponsored video begins.”

EvanTube agreed that, going forward, newly created sponsored videos will include an oral disclosure that the video is an “ad” or “advertising.”

To read CARU’s press release, [click here](#).

**Why it matters:** CARU noted that as the legal landscape continues to evolve and develop, the case presents novel and important issues for online advertisers and content creators that double as social media influencers. “The question of how to inform consumers that native ads are advertising, and not content, is a complex one, even for adults,” the self-regulatory body wrote. CARU emphasized that, since the FTC has made it clear that ads must be clearly disclosed and that the impact of the ad’s format on consumers will be considered, “it is imperative to adequately disclose the presence of advertising to children who are less sophisticated than adults.”

## Kardashians Accused of Failing to Keep Up With FTC Regulations

September 08, 2016

**The Kardashians are making headlines again, this time for allegedly violating the Federal Trade Commission guidelines on endorsements and testimonials in advertising.**

After reviewing the Instagram accounts of the Kardashian daughters, Truth in Advertising sent a letter to matriarch Kris Jenner and the family's lawyer stating: "We have found that members of the Kardashian/Jenner family are engaged in deceptive marketing campaigns for various companies by routinely creating and publishing sponsored social media posts for such companies without clearly and conspicuously disclosing that they are paid representatives of those companies or that the posts are advertisements."

After checking out the accounts for Kim, Khloe, and Kourtney Kardashian as well as Kylie and Kendall Jenner, the group found "a plethora of posts that do not clearly or conspicuously disclose their relationships with the companies being promoted in the posts as is required by federal law."

For example, Kylie Jenner posted a picture of her holding a Fit Tea product with the caption "using @fittea before my shoots is my favorite." Her Instagram post does not indicate that it is an advertisement, although the same picture is featured on Fit Tea's Instagram account.

In addition to Fit Tea, Truth in Advertising included a list of 27 companies—such as Estee Lauder and Puma—that were featured in similarly questionable posts by the Kardashian/Jenner sisters. The group requested that the posts be corrected to disclose material connections between the family and the companies.

When the Kardashians failed to satisfactorily respond, Truth in Advertising made a formal complaint to the FTC based on the allegedly deceptive native advertising by the family. At the same time, the Kardashians corrected 21 transgressions to include "#ad" at the beginning of the caption, they edited 6 to include an ad hashtag at the end of the caption, and they removed 4 from publication.

However, 75 others remained unchanged and 2 were "insufficiently edited" by adding "#spon" at the end of the post captions, Truth in Advertising told the FTC. "The willingness of the Kardashians/Jenners to alter their Instagram posts ... suggests that they would also fix other similarly deceptive posts if permitted to do so by the other companies they endorse," the complaint said. "As such, it is apparent that the issue is with the companies, who continue to flagrantly ignore the law." The group also noted that an additional 20 ads were found lacking disclosures during a second review.

The letter suggested the FTC take "appropriate enforcement action against those companies and individuals found to be violating the law," with an eye toward making sure "that all future social media posts promoting companies are properly and clearly labeled as advertisements."

The family's attorney informed Truth in Advertising that the women are "working diligently" to fix the challenged posts and "will make every effort" to ensure that future posts will include clear and conspicuous disclosures where appropriate.

The letter suggested the FTC take "appropriate enforcement action against those companies and individuals found to be violating the law," with an eye toward making sure "that all future social media posts promoting companies are properly and clearly labeled as advertisements."

To read the Truth in Advertising letter to Kris Jenner, [click here](#).

To read the Truth in Advertising complaint to the FTC, [click here](#).

**Why it matters:** Whether the FTC elects to launch an investigation into the high-profile celebrity family and its social media posts remains to be seen. Truth in Advertising's challenge is not the family's first run-in with this issue. Last year, pharmaceutical company Duchesnay received a warning letter from the Food and Drug Administration after a Kim Kardashian Instagram post included a photo of the reality star holding a bottle of its morning sickness medication and a post that read in part: "OMG. Have you guys heard about this?"

## NAD Recommends Goop Lifestyle Blog Clean up Its Claims

September 08, 2016

**Gwyneth Paltrow's agreement to discontinue her lifestyle blog Goop for a line of dietary supplements following an inquiry by the National Advertising Division provided an important reminder about endorsements.**

Her decision follows NAD's recommendation that Moon Juice discontinue certain claims for its drinks such as "Action Dust" and "Brain Dust," which were touted as "Designed to support peak performance, stamina, and longevity," "All Organic or Wild," and "Medicinal Grade" Moon Juice complied.

The same claims also appeared in the Goop blog where Paltrow was featured prominently throughout the site. Earlier this year, she also recommended that Moon Juice products be included in "GP's Morning Smoothie." According to the site, "Gwyneth drinks one of these every morning, whether or not she's detoxing. Choose your Moon Juice dust depending on what the day ahead holds ... brain before a long day at the office, sex dust before a date, etc."

Each of the Moon Juice products listed in the recipe included a hyperlink to a separate page on the Goop website where consumers could purchase the product. The purchasing page featured the same claims challenged by the NAD in the Moon Juice action.

"The product efficacy claims on the Goop website and Ms. Paltrow's endorsement of the products impose an obligation on Goop as a marketer to verify that the products provide the benefits it claims," the self-regulatory body wrote. "When marketing products for sale, an advertiser has an obligation to insure that the claims it makes for the product are truthful, accurate, and not misleading. The obligation to insure that advertising claims are truthful extends beyond the manufacturer of the product to affiliates who market the product."

Goop's claims about the Moon Juice dietary supplements "amplified" the target audience for the products, the NAD said. "The advertising marketplace is changing and advertisers are increasingly using third parties, including endorsers, influencers, and affiliate marketers, to reach consumers. It is equally important that such third-party marketing claims be truthful, accurate, and not misleading."

Goop represented that the Moon Juice advertising had been voluntarily and permanently discontinued and the NAD closed its inquiry.

To read the NAD's press release about the case, click [here](#).

**Why it matters:** Its concern regarding dietary supplements and Paltrow's apparent endorsement of the products prompted the NAD to remind advertisers that the obligation to ensure that advertising claims are truthful extends beyond the manufacturer to affiliates who market the product. As the role of influencers in social media increases, advertisers must remain cognizant that their advertising must be "truthful, accurate, and not misleading" and compliant with the Federal Trade Commission's Guides Concerning the Use of Endorsements and Testimonials in Advertising.

## Consumer Groups Urge FTC Action on Influencers

September 22, 2016

**Consumer groups are urging the Federal Trade Commission to review comments by social media influencers for possible violations of the agency's guidance regarding nondisclosed native advertising.**

Public Citizen, the Center for Digital Democracy, and the Campaign for a Commercial-Free Childhood sent a letter to the FTC's Bureau of Consumer Protection expressing concern "that the agency is failing to keep pace with developments in the social media space." Companies are routinely paying "influencers"—or social media users with a large following—to post endorsements of their products without disclosure, particularly on Instagram.

"A long-standing, core principle of fair advertising law in the United States is that people have a right to know when they are being advertised to," the groups wrote. "[D]isguised advertisements are inherently deceptive, because consumers do not know to apply appropriate screens. The issue is acute with disguised ads featuring paid endorsements, where deceived consumers believe admired celebrities are making genuine, self-directed and enthusiastic endorsements of brands, not realizing that those celebrities are instead paid and may not even use the touted brand."

Public Citizen conducted an investigation of the disclosure practices among movie stars, reality TV personalities, famous athletes, fitness gurus, fashion icons, and pop musicians and quickly found 113 influencers "who endorsed a product without disclosure." These noncompliant posts, including those from Rihanna to Victoria Justice, are not outliers, the groups wrote, adding that the cosmetics and weight-loss industries are prominent users of influencers.

The FTC needs to take action, and fast, the letter said. It encouraged the agency to investigate the current practices and take "aggressive enforcement action" against those that continue to engage in the practice of nondisclosed influencer advertisements.

The letter also suggested that the agency begin its work by taking a closer look at products such as Flat Tummy Tea and companies such as L'Oreal USA. While the groups said the emphasis of enforcement activity should focus on advertisers, "the agency should also communicate with prominent influencers, especially the highest-compensated among them, and warn them that they too will be subject to enforcement action for future non-compliance with FTC rules."

"The very viability of FTC fair advertising rules is at stake," the letter stated. "Consumer deception through hidden advertisements is now pervasive in social media, particularly on Instagram. It's past time for the FTC to bring the industry into compliance with the law."

To read the letter from the consumer groups, click [here](#).

**Why it matters:** The groups expressed concern that social media norms have already sufficiently evolved so that advertisers routinely contravene FTC policies as a non-objectionable matter of practice. "An important part of an FTC initiative must be to shift the center of gravity on social media so that advertisers take affirmative steps to ensure they comply with FTC rules designed to protect consumers from trickery and deception," according to the letter. "This problem has reached epidemic proportions. One agent who casts influencers estimates that there are 100,000 Instagram 'influencers' paid to endorse, a vast majority of whom do not disclose their advertisements."

## Study Finds Low Compliance for Native Advertising

April 28, 2016

**According to a new study, roughly 70 percent of websites are not compliant with the Federal Trade Commission's recently released native advertising guidelines.**

Last December the agency issued Native Advertising: A Guide for Businesses, in which it stated that consumers must be able to quickly and easily distinguish sponsored content from content that is independently created and produced. The FTC provided detailed recommendations as to how the necessary disclaimers must appear so that consumers know before they choose to view a native ad that it is commercial in nature. Ads that fail to do so are presumptively deceptive, the agency said.

To gauge compliance over the last few months, MediaRadar reviewed thousands of native ads and found that just 33 percent of publishers are currently labeling them in compliance with the FTC's guidance. Roughly 12 percent of the ads contained no label at all.

For those publishers that did label native ads, 54 percent used the term "sponsor" or "sponsored." Other popular terminology included "promoted," found on about 12 percent of the ads, and the word "ad" itself, used on approximately 5 percent of the sites. Less than 5 percent contained phrases such as "brought to you by," "partner content," or "content by."

Even publishers that applied a label failed to achieve compliance, because often the labels were either in the wrong place or were too subtle to be noticed by consumers, MediaRadar found.

The study also considered which industries favor native advertising. While the use of such ads is growing in general, the apparel and accessories category increased the most (up 82 percent from 2014 to 2015), followed by financial and real estate, food, and retail and travel, all with about 30 percent more native ads over the prior year.

"One of the reasons native is so fascinating is because it means many different things to publishers," according to the report. It noted that it tracked "almost 40 different implementation styles. Some are clearly identified, but others are extremely difficult to know that they were sponsored in any way."

**Why it matters:** The study demonstrates that advertisers are still struggling to achieve compliance with the FTC guidelines released little more than three months ago. However, the agency has already taken enforcement action, settling a case with Lord & Taylor. The department store chain launched an advertising campaign to promote its private-label clothing brand, using branded blog posts, photos, video uploads, native advertising editorials in online fashion magazines, and online endorsements by a team of specially selected "fashion influencers." The FTC said the company failed to disclose that the native articles and posts were paid commercial content and the fashion influencers failed to disclose they had been paid by Lord & Taylor and received free product.

## SPECIAL FOCUS: Lord & Taylor Settles With FTC for Not Disclosing Native Ads

March 16, 2016

By Lauren B. Aronson and Linda A. Goldstein

Less than three months after the Federal Trade Commission issued its December 2015 Policy Statement and Business Guide on native advertising (Native Advertising Guidance), the Commission has announced its first enforcement action and settlement in a native advertising case with department store chain Lord & Taylor. The action stems from a highly successful social media campaign launched by Lord & Taylor to promote its private label clothing brand Design Lab. The campaign included branded blog posts, photos, video uploads, native advertising editorials in online fashion magazines, and online endorsements by a team of specially selected "fashion influencers." According to the FTC, Lord & Taylor failed to disclose that the native articles and posts were paid commercial content and the fashion influencers failed to disclose that they had been paid by Lord & Taylor and received free product. Thus, because the case involves compliance with both the FTC's native advertising guidelines and the Testimonial and Endorsement Guides, it provides important lessons for marketers utilizing any form of native advertising or more broadly engaging in social influencer campaigns.

According to the FTC's complaint, Lord & Taylor engaged fashion magazines to produce native content designed to promote the Design Lab Paisley Asymmetrical dress. As part of the campaign, *Nylon*, an online magazine, posted a photograph to its Instagram account of the dress along with a caption. Lord & Taylor edited and approved the post without disclosing the commercial arrangement between itself and *Nylon*. Additionally, *Nylon* also ran an article regarding Design Lab, pre-approved by Lord & Taylor, without disclosing that the article was paid advertising content.

Furthermore, the FTC alleged that Lord & Taylor also engaged social media influencers to promote Design Lab on Instagram without ensuring compliance with the FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising. Lord & Taylor gifted the Paisley dress to 50 fashion influencers with sizeable social media followings and paid them between \$1,000 to \$4,000 to post stylish photographs of themselves wearing the dress on Instagram along with a caption. While the influencers were contractually obligated to mention and tag the company by using the user designation @lordandtaylor and to add the hashtag #DesignLab to the caption, they were not contractually obligated to disclose any material connection with the company. None of the posts disclosed that the dress was

given for free, that the influencer was compensated, or that the posts were part of a Lord & Taylor advertising campaign.

According to the FTC, Lord & Taylor's failure to disclose the commercial connections between itself and *Nylon* and the social media influencers communicated the false message to consumers that the Instagram images, captions and *Nylon* article were all independent content produced by unbiased consumers and an unbiased publication when in fact they were all part of Lord & Taylor's advertising campaign.

Not surprisingly, the *Proposed Consent Order*, which is up for public comment through April 14, 2016, prohibits Lord & Taylor from misrepresenting that "paid commercial advertising is a statement or opinion from an independent or objective publisher or source," that endorsers are independent users or ordinary consumers, or otherwise failing to disclose an unexpected connection with an endorser. Importantly, the Order also imposes significant compliance obligations on the company similar to those that the FTC imposed in a case brought several months earlier against Machinima. The company must:

- Provide each endorser with a clear statement of responsibility regarding disclosure obligations and obtain a signed and dated statement acknowledging receipt and agreeing to comply;
- Establish a monitoring system to monitor and review advertisements and communications made by endorsers as part of an Influencer Campaign; and
- Immediately terminate any endorser for misrepresenting impartiality or failing to disclose a material connection.

**Why it matters:** The FTC has made it clear that it is closely watching Influencer Campaigns and that advertisers are responsible for ensuring that material disclosures by endorsers—social media influencers and publishers—are clearly and conspicuously disclosed. Advertisers should take note of the obligations imposed on Lord & Taylor and consider incorporating the following requirements as they develop future Influencer Campaigns.

**Put Disclosure Obligations in the Contract.** Obtain a signed agreement from endorsers with a clear statement of responsibility and agreement to comply with disclosure obligations.

**Closely Monitor Endorsers.** Create a monitoring system designed to ensure that endorsers are properly representing their relationship to the advertiser and clearly and conspicuously disclosing the material connection.

**Training is Crucial.** Make sure that affiliates are trained to properly review sponsored content and endorsements.

**No Third Chances.** If an influencer makes a mistake and fails to adequately disclose a material connection, the advertiser may give them a second chance if the advertiser has reason to believe the failure to disclose was inadvertent. However, the advertiser must inform the influencer that they will be immediately terminated in the event of a subsequent compliance failure.



## FTC's Brill to Advertisers: Enhance Consumer Notice, Control

February 12, 2016

**Exhorting advertisers to provide consumers with greater notice and control—particularly with regard to native advertising and cross-device tracking—Commissioner Julie Brill of the Federal Trade Commission explained that traditional truth in advertising principles apply to 21st century technology.**

Speaking at the AdExchanger Industry Preview, Brill said it is clear that advertising is one of the most technologically advanced and data-driven industries in the economy today. "More than ever, advertisers leverage data to reach customers, personalize experiences, and predict consumer behavior," she noted. While the use of such data certainly has its benefits, Brill expressed concerns about consumer privacy and autonomy.

Despite the 21st century context, "the principles the FTC employs to protect consumer privacy and choice date back over 100 years," Brill told attendees, and the agency "has long believed that consumers must be given reasonable notice and control over how their personal data is collected and used—and that applies regardless of how many zettabytes of data we are talking about."

The Commissioner focused her remarks on two specific topics: the tracking of consumers, including cross-device tracking, and native advertising.

With regard to tracking—using sensors to follow mobile phone signals to detect individualized or aggregated traffic patterns as a consumer moves through a store or mall, for example—the bare minimum required of businesses is to give "relevant information about retail mobile location tracking when it is happening," and permit consumers "to exercise some control over its use," she said.

Brill referenced the FTC's enforcement action against Nomi Technologies to add that the choices provided to consumers must also be truthful. In that case, the company's privacy policy stated that it would "always allow consumers to opt-out of Nomi's service on its website as well as at any retailer using Nomi's technology," but the promised in-store opt-out mechanism was not available for nine months, the agency alleged.

Cross-device tracking magnifies privacy concerns, Commissioner Brill said, and it "is not clear that consumers are meaningfully informed about the cross-device tracking that's happening even today." She discussed the "troubling" findings of a recent agency look into cross-device tracking, where the FTC examined the top 20 websites in five different content categories. Although cross-device tracking mechanisms were employed at many of the sites, only a few provided an opt-out for consumers.

Lacking options and control, consumers will take matters into their own hands, as demonstrated by the rising popularity of ad-blocking technologies, she said. "It has surprised me that, so far, few advertisers seem willing to take up the offer to limit data retention, or to otherwise ensure consumers that they are treating their data properly," Brill said. "It's hard for me to believe that serving an ad while limiting data retention isn't better than serving no ad at all."

Turning to native advertising, the Commissioner reminded advertisers about the FTC's recent policy statement on the topic. She emphasized that advertising messages should be easily identifiable to

consumers as advertising and that "consumers should be able to recognize that content is sponsored before actually interacting with the content."

The policy statement "has roots in our past enforcement and policy efforts," where we address the tactics of door-to-door encyclopedia salesmen who misled consumers to think they had won a prize to get in the door or unsolicited e-mails with misleading header information designed to get consumers to open the message, Brill explained. "We will look at the entire ad to evaluate the net impression that the ad conveys to reasonable consumers," she said. "We also look to whether the consumer is misled to believe that a party other than the sponsoring advertiser is the source of the advertising."

In conclusion, Commissioner Brill noted that despite the explosion in technological sophistication in the advertising industry—and the agency's own technological capabilities—the principles of truth in advertising (consumers' choice over their data and privacy protection) still apply.

To read Commissioner Brill's prepared remarks, [click here](#).

**Why it matters:** "I urge you to continue to explore the creation of innovative and usable tools to address consumer concerns about privacy," Brill told her audience. "Not to find ways to work-around consumer choice, but to provide consumers with something they clearly want: to see advertising that respects their privacy and that they can trust."

## SPECIAL FOCUS: FTC Issues Long-Awaited Native Advertising Guidance

December 23, 2015

**On December 22, 2015, the Federal Trade Commission ("FTC" or "Commission") issued long-awaited guidance on native advertising – commercial content designed with the look and feel of editorial content – and published its Enforcement Policy Statement on Deceptively Formatted Advertisements ("Policy Statement") and its Native Advertising: Guide for Business ("Business Guide")** In the Policy Statement, the FTC stated that it "has long held the view that advertising and promotional messages that are not identifiable as advertising to consumers are deceptive if they mislead consumers into believing they are independent, impartial, or not from the sponsoring advertiser itself." The statement reflects the FTC's earlier guidance regarding advertorials and infomercials, misleading door openers, and deceptive endorsements. The Commission made it clear that consumers must know at the outset whether a message is commercial.

However, the new guidance goes beyond simply reminding advertisers that commercial content must be identified as such. Instead, as discussed below, this latest guidance reflects the FTC's view that consumers must be able to quickly and easily distinguish sponsored content from content that is independently created and produced. The FTC makes clear that consumers must know before they choose to view a native ad that the content is commercial in nature and that failure to clearly disclose the commercial nature is presumptively deceptive. Importantly, the guidance also provides very detailed recommendations as to how those disclaimers must appear.

### When is a Disclosure Required?

Whether a natively formatted advertisement must contain a disclosure identifying it as commercial content depends on how reasonable consumers would interpret the ad in a particular situation. However, in the Policy Statement and Business Guide, the FTC identified only a handful of circumstances where disclosure likely would not be required:

- Disclosure is not required if it is inherently obvious that a natively formatted ad contains commercial content. For example, the Policy Statement gives the example of an article with the headline “Come and Drive [X] today” and an image of a sports car.
- Disclosure is not required for paid branded product placements in entertainment programming provided that (1) payment is unlikely to affect the consumer’s decision to view the programming and (2) no claim is made. Thus disclaimers are not required for paid product placements that we regularly see in movies.
- Disclosure is not required either before or after a consumer clicks on an article, even if the article is sponsored by a brand, if the article itself does not feature, depict or promote any of the brand’s products.

However, aside from these exceptions, the new guidance takes a sweeping view of advertising and accordingly, the accompanying disclosure requirements. In the Business Guide, the FTC provides numerous scenarios in which disclosure would and would not be required. Key recommendations include:

The more a native ad has a similar format appearance, format, and topic to surrounding editorial content, the more necessary a disclosure will be. The FTC gives the example of an article entitled “The 20 Most Beautiful Places to Vacation.” The article was not sponsored and featured 20 images of vacation spots. However, a resort hotel paid the publisher to add a 21st image to the article featuring one of its beach resorts. While no disclosure is necessary on the main page, before the consumer clicks on the article, a clear and prominent disclosure of the paid nature of the 21st photo is required.

Know the platform. Whether a disclosure is necessary may vary depending on the platform. Consider how consumers customarily interact with each website or program in which the content appears. While it may be obvious on some platforms that content is sponsored, consumers may be misled on other platforms or in other media.

It must be clear to consumers before they choose to view an ad that content is commercial. If you use a share feature to allow consumers to share your native ad, the accompanying link or image must make clear that the content is commercial. Likewise, where articles appear in content, recommendation widgets must disclose if the content is commercial. The FTC also clarified that links and other visual elements appearing in non-paid search results must also effectively disclose the commercial nature of content when the content appears to be editorial on its face.

Paid dissemination of an independent article by a company may require disclosure. The FTC gives the example of a car company that paid to disseminate an article ranking one of its cars as the “Best Hybrid.” Although the article itself was independently written and published, if the company pays to disseminate the article through a recommendation widget, the company must ensure that all express and implied claims about the company and its products are truthful, non-misleading, and substantiated. Furthermore,

the company should also disclose that the link on the recommendation widget was paid before consumers click on the link.

Disclosures may be required for branded product placements in entertainment programming – including video games, apps, social media videos, and television shows. Disclosure is required when objective claims or recommendations are made regarding a branded product and consumers would not realize that sponsors have paid for product placement. Notably, the recommendations do not need to be express – a recommendation could be made simply by zooming in on the sponsored product if consumers are likely to interpret the use of the product to be a recommendation and not a paid inclusion.

### **How Should Advertisers Make Clear and Prominent Disclosures?**

The FTC reiterated the basic principles of its 2013 guidance document “.com Disclosures: How to Make Effective Disclosures in Digital Advertising”. The guidance states that “Advertisers have flexibility as to how to identify native ads, as long as consumers notice and process the disclosures and comprehend what they mean.” However, not only should disclaimers be prominent and clearly understandable, the Business Guide also includes very specific guidance for placement that deviates from current industry practice. Key recommendations include:

Pay attention to how consumers view content on the website. Disclaimers must be placed where consumers look first. For example, if a webpage is read from left to right, consumers are less likely to notice disclosures placed to the right of the native ads. The Commission recommends that the disclaimer be placed close to the headline, on the left. Similarly, if native ads appear in a vertical stream of content items, the disclaimer should appear “immediately in front of or above a native ad’s headline.”

Don’t assume that it will always be sufficient to place a disclaimer in a headline. On some platforms, the FTC notes that focal points are images or graphics, not headlines or other written text. The FTC recommends that the advertiser place a disclosure directly on the image itself. This recommendation would likely apply to sponsored videos created by influencers on platforms such as YouTube.

However, when native content is only a small part of larger content (for example, one small element of a video that is primarily independent of the advertiser), the disclaimer must appear as close as possible to the advertising message. The FTC notes that it may be “problematic” to make a disclosure too early in a video if, for example, the sponsored content is simply a video vignette or game shown part way through the video.

When native ads appear alongside editorial content, the native ads must be easily identifiable. The FTC recommends against using a single disclosure to identify multiple native ads. The advertiser should use individual disclosures or, if a single disclosure is used, the advertiser should also use other visual cues (e.g., background shading or a clear outline or border) to make it obvious which items are native ads.

Advertisers must account for the effectiveness of disclosures when content is republished by others. The location of the disclosure may need to change, depending on how the content is shared. The FTC states that links shared on social media or email should include a disclosure at the beginning of the native ad’s URL.

Choose the appropriate disclaimer. While the FTC thinks “Ad,” “Advertisement,” “Sponsored Advertising Content” or similar are effective, the FTC states that “Promoted” or “Promoted Stories” are too

ambiguous. Furthermore, disclaimers such as “Presented by [X],” “Brought to You by [X],” “Promoted by [X],” or “Sponsored by [X]” may be insufficient if the advertiser created or influenced the content. In such cases, consumers may falsely believe that the advertiser solely paid to publish the content.

**Why it matters:** In 2016, the FTC will likely begin to aggressively monitor native ads, as it has aggressively monitored other forms of sponsored content. The Commission will likely bring carefully chosen native advertising cases to further elucidate and clarify its thinking in this area. As advertisers think about native advertising going forward, they should pay close attention to the FTC’s guidance when evaluating whether, when, where, and how to effectively disclose to consumers that content is sponsored. The FTC has made very specific recommendations regarding how and when disclaimers should appear that have important implications for both native advertising and sponsored content in social media more generally.

## Social Media

### Pin This: New Contest, Sweepstakes Rules for Pinterest

September 08, 2016

**Pinterest updated its Acceptable Use Policy recently to include changes as to how companies can conduct contests and sweepstakes on the social media site.**

Before the update, brands were prohibited from requiring entrants to Pin from a selection of options or requiring a minimum number of Pins to enter a promotion. Companies were also not allowed to conduct a promotion where each Pin, like, or board constituted an entry.

In its August 2016 update to the Acceptable Use Policy, Pinterest removed the prohibitions and instead added a new general recommendation to advertisers: "If you run a contest or other type of promotion on Pinterest, please encourage authentic behavior, keep Pinterest spam-free and be sure to comply with all relevant laws and regulations."

In addition, the policy established three rules that broadened the options for brands. Going forward, companies should not require participants to Pin a specific image. "Successful contests encourage creative and authentic behavior," the platform explained. "Give Pinners the ability to choose Pins based on their tastes and preferences, even if it's from a selection or a given website."

Next, Pinterest advised that participants should not be allowed more than one entry each. "Contests that incentivize users to submit multiple entries per person feel less authentic and can negatively impact other Pinners."

Finally, brands should not suggest that Pinterest is a sponsor or an endorser of their contests, they should not use the Pinterest wordmark, and they should keep the badge smaller in scale than the brand's own logo to avoid an implied endorsement.

To read Pinterest's Acceptable Use Policy, [click here](#).

**Why it matters:** Pinterest's new Acceptable Use Policy updates its guidelines for running contests and sweepstakes on the platform. While the platform no longer expressly prohibits sponsors from requiring participants to choose from a selection of Pins, the new Acceptable Use Policy underscores that promotions should be legally compliant and that they should encourage authentic and spam-free behavior.

### U.S. Olympic Committee Sued Over Social Media Olympic Rules

September 01, 2016

**Although the 2016 Summer Olympics have come to an end, the U.S. Olympic Committee is still facing a lawsuit accusing it of "exaggerating" the strength of its legal rights to the detriment of advertisers.**

Prior to the Olympics, the USOC cautioned businesses to avoid "social media posts that are Olympic themed, that feature Olympic trademarks, that contain Games imagery or congratulate Olympic

performance unless you are an official sponsor." It sent a warning letter to non-sponsor companies cautioning them against using the Olympics' trademarks, even in hashtags (such as #Rio2016 and #TeamUSA).

One company decided to fight back.

A small carpet cleaning business in Minnesota, Zerorez communicates with customers on Facebook and Twitter on a variety of topics including holidays, cleaning tips and pets. With the Olympics on the horizon, the company anticipated discussing the event, contemplating social media posts such as: "Congrats to the 11 Minnesotans competing in 10 different sports at the Rio 2016 Olympics! #rioready" and "Are any Minnesotans heading to #Rio to watch the #Olympics? #RoadToRio."

But when faced with the USOC's Olympic and Paralympic Brand Usage Guidelines—which cautioned advertisers about the Committee's marks in any form of advertising and stated that any use of the trademarks on a non-official sponsor site would be viewed as commercial in nature and consequently prohibited—Zerorez said it elected not to engage.

"But for the USOC's Actions, Policies, and threats, Zerorez would exercise its First Amendment rights by discussing the Olympics on social media," according to the company's Minnesota federal court complaint, arguing that the Committee violated the First and Fourteenth Amendments to the Constitution. "The USOC's Actions, Policies, and threats have had the effect of chilling, silencing, and censoring Zerorez's speech about the Olympics on social media."

Zerorez requested declaratory relief from the court in the form of an order that it "is possible for businesses, including those that are not official Olympic sponsors, to mention the Olympics, Olympic results, and Olympic athletes on social media without violating the legal rights of the U.S. Olympic Committee" and that the "mere mention of the Olympics, Olympic results, and Olympic athletes, by a business not sponsoring the Olympics is not necessarily a violation of the rights of the U.S. Olympic Committee."

To read the complaint in *HSK LLC v. United States Olympic Committee*, [click here](#).

**Why it matters:** The Olympics are over but the plaintiff's complaint argued that the action remains relevant for subsequent Olympic events, such as the Winter Olympics and the Paralympics. Plaintiff requested that the court recognize that the "USOC violated fundamental Constitution rights" and that "[s]peech is not commercial in nature merely because it is on a business's social media account."

## Twitter Seeks Ninth Circuit Ruling That It Does Not "Make" Calls

August 16, 2016

**After losing a round in a California district court, Twitter has appealed to the Ninth Circuit Court of Appeals from a ruling in a Telephone Consumer Protection Act case leaving the social network on the hook for unwanted text messages.**

Beverly Nunes sued the social media microsite in 2014 after she purchased a new cell phone and began receiving texts from Twitter. The prior owner of the phone number had subscribed to receive specific

notifications from various tweeters via text and Twitter continued to send them to Nunes after the number was reassigned.

Twitter mounted a two-pronged defense in its motion for summary judgment: first, that it was not the "maker" of the texts under the TCPA, and second, that it was immunized from liability under the Communications Decency Act (CDA). In declaring both of the arguments "wrong," U.S. District Court Judge Vince Chhabria granted summary judgment in favor of Nunes.

The defendant's contention that it does not "make" the tweets at issue is contrary to the language of the statute, the ordinary meaning of the word "make," and the purpose behind the TCPA, the court said. "The statute says it is unlawful 'to make any call' to a cell phone using an 'automatic telephone dialing system' without 'the prior express consent' of the recipient of the call," the court explained. "In the circumstances presented by this case, Twitter is the only conceivable 'maker' of any of these calls."

Twitter is the one alleged to have used an ATDS to send the text messages to the recipient and "is the actual sender of the text," Judge Chhabria wrote. The author of the tweet "cannot possibly" be the maker of the call, because under Twitter's default setting, the author does not control who may sign up to receive his or her tweets and is not involved in the mechanics of actually transmitting any text messages.

The defendant posited that the former owner of the phone number who signed up to receive tweets was the "maker" of the text messages to that number in the future. Twitter argued that by signing up to receive tweets via text message, the former owner "initiated" all text messages sent by the social networking site, relying upon a 1991 ruling from the Federal Communications Commission that used the word "initiate" in certain instances to refer to "making" a call.

"But the FCC's ruling contemplates merely that a person can be deemed to have 'made' or ('initiated') a call if he was heavily involved in the 'placing' of a 'specific' call," the court said. "There is no suggestion that a person can be the 'maker' of the call if he merely signed up to receive any unspecified number of calls in the future, and as previously noted, such an interpretation would be contrary to the plain meaning of the statute."

Judge Chhabria distinguished an FCC ruling on group messaging services, finding that in contrast to that app, where the user invites people to sign up for the service, "the new owner of a recycled number is receiving tweets via text message [but] the former owner of the number is not 'placing' any 'specific' calls to her. He can't be, because he likely doesn't know when (or even if) the person whose tweets he signed up to receive via text message will compose a tweet. Nor does he know, once he relinquishes his number, to whom (if anyone) new text messages will be sent."

Consideration of the goals and purposes of the TCPA only weakened Twitter's argument even more, the court added, particularly in the wake of the FCC's 2015 [Declaratory Ruling](#) finding that the caller—and not the wireless recipient of the call—bears the risk that the call was made without the prior express consent required under the statute.

"It may be true, as Twitter argues, that it's presently difficult or impossible for companies to detect when they are sending out texts to people with recycled numbers," the judge wrote. "But as the FCC noted, there are apparently many steps businesses can take to identify reassigned numbers. And if Twitter's proposed interpretation of 'make any call' were to prevail, the owners of recycled numbers who receive



unwanted tweets via text message would have no protection under the TCPA. That conclusion, in addition to being contrary to the text of the statute, would be in sharp tension with the FCC's 2015 decision about how to implement the TCPA when recycled numbers are involved, and its discussion of how the statute's purposes should be effectuated."

The court also determined that the CDA does not shield Twitter from potential liability under the TCPA, as the site does not review or edit the content of the tweets or make decisions about whether to send out a tweet.

"Nunes' claim against Twitter under the TCPA does not depend on the content of any tweet, or on any assertion that Twitter is required to sift through content to make sure the content is not bad," Judge Chhabria said. "Just the opposite—if Twitter ends up being liable under the TCPA, it would be liable whether the content of the unwanted tweets is bad or good, harmful or harmless. Either way, the unwanted tweet is a nuisance."

Twitter quickly responded with a motion to certify Judge Chhabria's order for interlocutory appeal to the Ninth Circuit, arguing that the ruling involved a controlling question of law on the proper interpretation of the FCC's 2015 Ruling on a matter about which reasonable jurists could disagree and have disagreed.

"Several courts have already rejected claims against online services similarly situated to Twitter, on the grounds that a service that transmits user-directed messages does not initiate them within the meaning of the FCC order," the company wrote in its motion for certification, citing decisions from courts in California, Illinois, and Florida.

These other courts read the FCC Ruling as making the determination whether an intermediary service makes or initiates the text messages it transmits turning on factors identified by the agency, such as whether the service or its user determined whether, when, and to whom the messages would be sent, and who supplied the content, Twitter told the court. "These courts did not consider the identity of the recipient of a text message relevant to the question of who initiated the text message."

To read the order in *Nunes v. Twitter, Inc.*, [click here](#).

To read Twitter's motion for certification to appeal the order, [click here](#).

**Why it matters:** The district court took particular issue with Twitter's stance that the ruling would leave the company no choice but to stop sending its text messages. "The implication seemed to be that this result would be unbearable," Judge Chhabria wrote. "[I]t's unclear why the desire to send alerts by text message (rather than email, or push notification through an app) should prevail over the TCPA's goal of protecting people with recycled numbers from receiving unwanted texts sent by companies using autodialers." In its motion for certification, Twitter noted that the issue is already pending before the Ninth Circuit, suggesting that the federal appellate court combine its case with the other "to ensure that the Ninth Circuit considers the meaning of the FCC Order comprehensively, with a broader appreciation of the scope of the precedent." The issue "is vital given the ever-growing number of modern communications technologies, and the explosion of TCPA litigation nationwide," Twitter added.

## First Circuit Affirms Ruling Against [Jerk.com](#)

June 02, 2016

**In a victory for the Federal Trade Commission, the First Circuit Court of Appeals affirmed a Commission ruling that website [Jerk.com](#), a self-described reputation management website, ran afoul of Section 5 of the Federal Trade Commission Act by misrepresenting the source of its online profiles and the benefits of membership.**

[Jerk.com](#) posted profiles of persons for which users could cast a "jerk" or "not-a-jerk" vote. Although [Jerk.com](#) maintained that users created the profiles, in reality, the site swiped data and pictures from other social networks to create the majority of the "jerk" profiles and promised that individuals could "manage [their] reputation and resolve disputes" by purchasing a subscription for \$30, the FTC said. The agency moved for summary decision and the Commission granted the motion on both counts, finding founder John Fanning personally liable for Jerk's misrepresentations.

The Commission entered an order enjoining the defendants from making certain misrepresentations and imposing monitoring and recordkeeping requirements. Fanning appealed.

While the First Circuit agreed with Fanning that portions of the Commission's order were overbroad, it affirmed the finding of liability as well as the recordkeeping and order acknowledgment provisions.

The appellate panel considered the "overall net impression" of the claim that Jerk.com's profile pages were user-generated, and found the claim to be material and deceptive. For example, the site referenced its "millions" of users, and [Jerk.com](#) contained a disclaimer that it could not be held liable for content because it reflected the views of those users. Combined with other statements made throughout the site (describing it as "a vibrant source of user participation and social interaction" with an open invitation to post profiles of other individuals), the court agreed with the Commission that consumers could be misled.

"[E]ven if [Jerk.com](#) never expressly represented that its profile pages were created exclusively by users, it never expressly stated how the pages were created," the First Circuit wrote. "Given Jerk.com's emphasis on user-generated content and the lack of information to the contrary, reasonable consumers could conclude other [Jerk.com](#) users created their profile pages."

The court similarly affirmed the Commission's holding with regard to the second count. "Two FTC investigators paid the \$30 membership fee and never received any communication from Jerk," the panel said, adding that the FTC received numerous complaints to the same effect. "[T]he record is bereft of any evidence that [Jerk.com](#) provided even one paid member the opportunity to contest information on a profile page," despite the defendants' promises to the contrary.

The court also said it found no merit in Fanning's objections to the injunction against making any misrepresentations about the "source of any content on a website" and "the benefits of joining any service." The First Amendment does not protect misleading commercial speech, the panel said, and found a "reasonable fit" between the FTC's restriction on the misleading speech and the government interest it served.

Recordkeeping provisions requiring Fanning to "maintain" and "make available" advertisements and promotional materials for a five-year period and notify the Commission of any complaints or inquiries

relating to any website or other online service were also reasonably related to the defendants' FTC Act violations, the court determined. Both were tied to "misrepresenting the source of Jerk.com's content and the benefit of its membership subscription," the court wrote, particularly given the ease with which Jerk.com's practices could be transferred to other websites.

However, the First Circuit agreed with Fanning that the compliance monitoring requirement—mandating that he notify the Commission of "his affiliation with any new business or employment" for a period of 10 years—was not reasonably related to his violation. "Fanning must notify the Commission of all business affiliations and employment—regardless of whether or not the affiliate or employer has responsibilities relating to the order," the panel said. While the FTC told the court that it has traditionally required such reporting, the Commission also conceded that the provision would require Fanning to report if he were a waiter in a restaurant.

Affirming the other parts of the order, the First Circuit vacated and remanded the compliance monitoring requirements.

To read the opinion in *Fanning v. FTC*, [click here](#).

**Why it matters:** The FTC hailed the First Circuit opinion. "This ruling makes it clear that the defendant's misrepresentations in this case were harmful to consumers," Jessica Rich, Director of the agency's Bureau of Consumer Protection, said in a statement about the decision. "We are pleased with the ruling, and will closely monitor the defendant's compliance with the order, as we do in all our cases." For advertisers, the decision reiterates that the FTC can find deception based on the "overall net impression" presented by a website and not simply express claims.

## Mobile Marketing

### Ninth Circuit: Confirmation Text Message Doesn't Violate TCPA

October 18, 2016

**The Ninth Circuit Court of Appeals has upheld dismissal of a class action seeking to hold a defendant liable under the Telephone Consumer Protection Act for a confirmation text message.**

Eric Aderhold registered to use the car2go service and provided the company with his cell phone number. As part of the registration process, he received an automated text message to his cell phone requiring him to enter a validation code on car2go's Web site.

Aderhold sued, alleging that the text violated the TCPA. A district court dismissed the suit and the plaintiff appealed.

The Ninth Circuit sided with the defendant for two reasons.

First, Federal Communications Commission regulations dictate such an outcome, the three-judge panel said. The agency's 1992 rules state that "persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary."

"Aderhold therefore consented to receive text messages related to the application process from car2go simply by providing his phone number in the application for membership," the court wrote. It found that this submission of information by the plaintiff satisfied the circuit's standard that "prior express consent" be "[c]onsent that is clearly and unmistakably stated."

As a secondary reason for tossing the suit, the Ninth Circuit said the text received by Aderhold was not a "telemarketing" message. "A message is characterized as 'telemarketing' if it is issued 'for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services,'" the court said, adding that it approached the question of a message's purpose "with a measure of common sense."

"Car2go's message contains no content encouraging purchase of car2go services," the panel wrote. "The message was directed instead to completing the registration process initiated by Aderhold and to validating personal information. We follow the FCC's determination that such messages, 'whose purpose is to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender are not advertisements.'"

To read the memorandum in *Aderhold v. car2go, LLC*, [click here](#).

**Why it matters:** The Ninth Circuit affirmed the district court's "common sense" approach to the question of consent, finding it axiomatic that if a consumer provides a cell phone number as part of the registration process, he has signaled his consent to receive text messages at that number. The panel further found no merit to the argument that every message sent from a business constitutes telemarketing, and ruled that because car2go's message was directed to completing the registration process—initiated by the plaintiff—no liability under the TCPA attached to the text.

## SPECIAL FOCUS: Responses to Retail Webinar Attendee Questions

September 20, 2016

By Marc Roth

**During our hugely successful “Avoiding TCPA Pitfalls: Essential Guidance for Retailers” webinar this summer, we received dozens of questions from attendees, most of which we were not able to address during the closing minutes of the presentation. But, we held on to the questions and present below responses to those that we felt would be most relevant to readers. Please note that these are general responses and are not intended as, and should not be construed to be, specific legal advice. Should you have any specific follow-up questions on these responses, please reach out to the editors.**

**Q: I thought mobile phones always trigger the TCPA even if manually dialed? Especially in certain states?** Not exactly. The TCPA is only triggered when communicating with consumers on their mobile phone when using an autodialer. That said, the FCC’s July 2015 rulemaking declared that a dialing system that is used to manually dial numbers may be an autodialer if it has the current or future capacity to autodial. With regard to state laws, there are about half a dozen states that prohibit calling or texting a mobile device without the consumer’s consent, regardless of whether an autodialer is used. But this restriction only applies to commercial, and not informational or transactional, communications.

**Q: If there is time, could you please address TCPA applicability to texts delivered to cell phones?** The FCC has expressly stated that text messages delivered to cell phones are treated as calls under the TCPA.

**Q: If you use a prerecorded message that is only informational in nature (e.g., fraud prevention), does prior express consent need to be obtained?** It depends on where the call is terminated. If the call is to a landline and contains no marketing content, no consent is required. On the other hand, if the call is to a mobile phone, and is purely informational, the caller will still need the recipient’s express consent, which may generally be satisfied by the caller receiving the number from the call recipient.

**Q: Do autodialed calls to mobile numbers assigned to a business fall under the TCPA? For calls to “residential” numbers, can we assume “residential” means a call to a consumer landline phone?** Unless expressly exempted, all autodialed calls to a mobile phone require some level of consent, even if to a business. The TCPA and FCC rules do not distinguish between consumer and business lines when calling mobile numbers. This distinction is only relevant in regard to do-not-call regulations, since these rules only apply to consumer numbers. However, as some people use a single phone line for both personal and business purposes, a more detailed analysis of the source and use of the number is required in order to determine whether the DNC rules apply.

**Q: Is the company required to determine whether the consumer’s phone number is a landline or cell phone? Or is this information provided by the consumer?** A company must itself determine whether a number terminates with a landline or mobile phone. As the TCPA is a strict liability statute, even if a consumer provides her mobile phone number in response to a request for a home (landline) phone, a call to that number will still be treated as a call to a mobile device under the TCPA.

**Q: Can voice recordings giving consent to be marketed (via inbound call) comply with the ESIGN Act?** Yes, under FCC rules, a company may obtain a consumer's express written consent for marketing calls via an inbound call if conducted in accordance with the requirements of the ESIGN Act.

**Q: Does a check box work as a signature for prior express written consent (PEWC)?** A check box may satisfy the FCC regulations for prior express written consent if the box is unchecked and is accompanied by the applicable FCC consent language in accordance with the ESIGN Act.

**Q: Is it imperative to be able to store and produce (if need be) the check box that is used for the consumer to affirmatively agree to receive telephone calls?** It is important to maintain some proof of a consumer opt-in in the event a call is ever challenged. While the best proof may be a copy or screenshot of the exact web page a consumer completed and submitted for this purpose, if this is impossible, it may be acceptable to maintain a file of the opt-in that includes the information that the consumer provided as well as a date and time stamp of and IP address associated with the opt-in.

**Q: A retailer announces via the in-store intercom: text COUPON to 12345 to get 10% off your purchase today. Is this allowed? Can the response include an invitation to subscribe via web form, e.g., Your 10% off code is XYZ. Click to subscribe: bit.ly123?** Under the FCC's July 2015 ruling, a retail store may instruct consumers to text a word to a short code to obtain a discount code by reply text without including the required language for prior express written consent. Under the FCC rules, the reply text must only contain the requested information (i.e., the discount code) and may only be used once. Including any other information in the reply text (such as an invitation to subscribe to the retailer's savings or loyalty program via a web link) may present some risk as such content may be viewed as exceeding the consumer's specific request.

**Q: What are your thoughts on placing express written consent language below a "submit" button?** The FCC regulations require that express written consent language be presented clearly and conspicuously so that it is not missed by consumers. Placing this language below a submit button presents some risk of not satisfying this requirement if displayed in a way that may be missed by the consumer.

**Q: Does consent override DNC? For example, customer gives PEWC on retailer website but that number is also listed on the national DNC.** It depends. If the PEWC language makes clear that the consumer is agreeing to receive marketing communications to a telephone number that is on a DNC registry, then yes, the consent will override the registry listing.

**Q: What about making service calls to numbers on an internal DNC list?** Pure service calls are exempt from the internal DNC regulations. DNC applies only to marketing calls.

**Q: If customers provide PEWC after their request to be added to the internal DNC registry, should they be removed from the internal DNC registry?** The PEWC opt-in may, depending on its wording and the context in which it was given, trump the internal DNC request.

**Q: Does affirmative agreement need to specifically state "I agree/consent" or does something like "reply YES to receive msgs" constitute an affirmative agreement for text messages?** The TCPA and FCC regulations do not specifically dictate the precise language that must be used to obtain a

consumer's express opt-in. But the language must clearly and unambiguously reflect the consumer's desire to opt in.

**Q: Are text messaging platforms liable under the TCPA?** They are just message conduits. A number of courts have held and the FCC has ruled that texting platforms will not be liable under the TCPA as the "maker of a call" in certain circumstances, particularly when users of the platform (and not the platform itself) control the content and transmission of the messages. Said otherwise, the more involvement a platform operator has in the message development and transmission process, the greater chance it may be found responsible under the TCPA.

**Q: With text messages, can the consent be asked for in that first text for future texts or does that bump it out of the exception?** If you are referring to the one-time exception to respond to a consumer's specific request, the FCC was pretty clear in its rulemaking that the one-time response must only include content that responds specifically to the consumer's request. That said, the ruling responded narrowly to a petition that sought the one-time exception for a single purpose, so it remains unclear whether seeking additional consent would be acceptable. On balance, given the risks associated with violating the TCPA, it would be prudent to only include responsive content.

**Q: Do you need consent to make a marketing call without an autodialer? What if you don't know if it is a mobile or landline phone?** As noted above, the onus is on the caller to determine whether a number is associated with a mobile or landline phone. Relying on how a consumer identified her number is not a defense to liability under the TCPA. If a marketing call is made without an autodialer and does not introduce a prerecorded message, no consent is required for TCPA purposes, but certain states do still require a consumer's consent.

## ***Spokeo, Inc. v. Robins: What Does It Mean for TCPA Lawsuits?***

May 24, 2016

By Christine M. Reilly | Marc Roth | Diana L. Eisner

**As reported in our recent [TCPA Connect](#), on May 16 the United States Supreme Court issued its highly anticipated ruling in *Spokeo, Inc. v. Robins*. The High Court ruled that a plaintiff must show a "concrete" injury-in-fact to pursue a claim arising under the Fair Credit Reporting Act (FCRA). However, the Court's reasoning was not confined to FCRA and its decision will likely have far-reaching implications in a variety of class action lawsuits brought under other federal consumer protection statutes, including the Telephone Consumer Protection Act (TCPA).**

As the Court recognized, "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation." Alleging a "bare procedural violation" of a statute is insufficient to confer standing where there is no real harm.

At the pleading stage, then, the plaintiff must "clearly allege facts" demonstrating a concrete injury. "Concrete" means that the injury must be "real" and not abstract; in other words, an injury must "actually exist." However, the Supreme Court left open the possibility that the "violation of a procedural right

granted by statute can be sufficient in some circumstances to constitute injury in fact." In such a case, a plaintiff need not allege any additional harm beyond the one identified by Congress.

It remains to be seen how *Spokeo* will be applied in TCPA cases, but *Spokeo* certainly adds to a defendant's arsenal of arguments designed to dispose of a case at an early stage and may help curb the explosion of TCPA lawsuits over the last several years. TCPA plaintiffs and their attorneys often take a "kitchen sink" approach to litigation and pursue TCPA lawsuits in mass volume. Complaints are typically boilerplate, containing minimal, if any, connection between the defendant's alleged violation and any actual injury. Thus, many plaintiffs pursuing claims under the TCPA do not allege a "real" injury, other than a violation of a statutory right.

In the "robocall" context, for example, many plaintiffs simply allege receipt of an unwanted call or text message. Other plaintiffs acknowledge they consented to receive text messages, but the messages do not contain the precise disclosure language required by the FCC's regulations. Now, after *Spokeo*, it is possible that such allegations cannot ipso facto establish standing to sue. Plaintiffs may need to allege a concrete or real harm. This may be difficult, given that so many Americans are on "unlimited" or flat-rate cell phone plans where no charges are incurred for incoming calls or text messages and no other "injury" exists other than an alleged privacy invasion. In cases where the plaintiff did not answer the phone or know about the call absent the use of Caller ID, the plaintiff may be unable to allege a concrete harm stemming from the unanswered call, potentially shuttering the lawsuit.

In the fax context, TCPA plaintiffs often allege that the opt-out notice on junk faxes does not comply with the TCPA's technical requirements, including the specific disclosure that failure to remove the recipient from the distribution list within 30 days of receipt of the opt-out request violates the law. Complaints are usually devoid of any alleged harm stemming from this type of technical violation, particularly where the fax otherwise contains opt-out instructions. Before *Spokeo*, this allegation may have been sufficient to establish Article III standing, despite the absence of any alleged concrete harm to the recipient. Now, this type of allegation may very well be insufficient to confer Article III standing, given the lack of any alleged harm from what appears to be a "bare procedural violation."

Importantly, standing under Article III of the U.S. Constitution is a threshold requirement to bringing suit in federal court—a plaintiff without Article III standing cannot maintain suit. Moreover, this jurisdictional issue can be raised at any time, including on appeal. So, even for defendants currently engaged in TCPA litigation, *Spokeo* may provide another avenue for limiting or disposing of TCPA cases.

Beyond the threshold standing issue, *Spokeo* has the potential to constrain a plaintiff's ability to certify a class under Rule 23 of the Federal Rules of Civil Procedure. Under Rule 23, the primary inquiry is whether questions of law or fact are common to all class members. If commonality is lacking, no class can be certified. In TCPA cases, plaintiffs have obtained class certification based on the mere receipt of an alleged call, text message, or fax giving rise to a cause of action. However, based on *Spokeo*, arguably each class member must demonstrate a concrete harm, which may create an individualized inquiry that is inapt for class resolution.

In practice, *Spokeo* may force plaintiff lawyers to select putative class representatives more carefully, and to ensure that the named representative has suffered a "concrete" injury from a purported violation. *Spokeo* could also curb federal lawsuits based solely on a technical violation of the TCPA, such



as an insufficient or imperfect disclosure. And, given the potential impact on class certification under Rule 23, narrowed class definitions could become the trend. TCPA classes are typically broadly defined and include all persons who received the alleged call or text during the four-year statute of limitations. Class composition could shift from a class that includes everyone on the defendant's call log to a class composed only of those who have suffered specified injuries.

As this decision promises to have significant implications for TCPA litigation, members of Manatt's TCPA Compliance and Class Action Defense practice will continue to actively monitor developments in this area. For further information on this decision, please contact the authors of this newsletter noted above.

## **Prior Express Consent Exists When Cellphone Number Is Shared With Intermediary**

March 25, 2016

**Joining other federal appellate courts, the Sixth Circuit Court of Appeals recently held that prior consent that is provided indirectly to a third party can be deemed express consent for purposes of TCPA compliance.**

Two patients of Mount Carmel Hospital in Columbus, Ohio provided their cellphone numbers while completing authorization forms for medical care. Zachary Baisden agreed that Mount Carmel could use his "health information" for "billing and payment" purposes, which information could be released in a variety of forms, from electronic to verbal. Brenda Sissoko signed a different version of the form, permitting the release of her health information whether in electronic, written, or verbal form "to companies who provide billing services for physicians or other providers involved in my medical care."

Baisden and Sissoko owed \$850 and \$444.94, respectively to Consultant Anesthesiologists, which provided anesthesiology services to Mount Carmel. Consultant transferred their delinquent accounts to Credit Adjustments. The debt collector called their cellphone numbers in an attempt to collect on their accounts.

In response, Baisden and Sissoko filed suit. Because they never provided Credit Adjustments with their cellphone numbers, they claimed the debt collector violated the TCPA by calling them. Credit Adjustments moved for summary judgment, arguing that by providing their numbers to the hospital where they received medical care, the plaintiffs gave their prior express consent to receive such calls.

A federal district court agreed that the necessary consent can be provided indirectly and a panel of the Sixth Circuit affirmed.

The Federal Communications Commission has provided "extensive" guidance on what constitutes prior express consent, the court explained, referencing four interpretations pertinent to the case. In 1992, the FCC interpreted prior express consent to include a form of implied consent in a Report and Order, writing that "persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary." For support, the agency relied upon the TCPA's legislative history.

In 2008, the FCC extended this proposition to cellphone numbers in a Ruling that placed the burden on callers to demonstrate that consent was provided. Applying both the 1992 Order and 2008 Ruling to intermediaries, a 2014 Declaratory Ruling from the FCC held "that the TCPA does not prohibit a caller ... from obtaining the consumer's prior express consent through an intermediary[.]"

Most recently, the agency's 2015 Order affirmed the 2014 Declaratory Ruling, and stated again that consent can be provided more than one way and that the context in which consent is provided is important.

The plaintiffs took a narrow reading of the FCC guidance, zeroing in on language in the 2008 Ruling that "prior express consent is deemed to be granted only if the wireless number was provided by the consumer to the creditor."

Relying heavily on an Eleventh Circuit decision with similar facts (*Mais v. Gulf Coast Collection Bureau Inc.*), the Sixth Circuit rejected the plaintiffs' interpretation of the FCC guidance as well as their objections to the *Mais* ruling.

Baisden and Sissoko argued that *Mais* was "seriously flawed" and enlarged the scope of the FCC rulings to read out the consumer protections found in the TCPA. But the court refused to opine on the validity of the FCC's rulings or ignore the agency's guidance. The 2014 Declaratory Ruling "stressed that 'allowing consent to be obtained and conveyed via intermediaries ... facilitates ... normal, expected, and desired business communications in a manner that preserves the intended protections of the TCPA.'"

The 2015 Order similarly stressed the importance of context when considering a consumer's consent, which depends on the facts of each situation, the court said. "[I]f one provides a cell phone number to a health organization seeking medical treatment, and a provider affiliated with that health organization treats that person for the same ailment, it is normal, expected, and desired to interpret that provision of the cell phone number as an invitation for an entity affiliated with that organization to call for something arising out of one's treatment."

"The FCC's rulings in this area make no distinction between directly providing one's cell phone number to a creditor and taking steps to make that number available through other methods, like consenting to disclose that number to other entities for certain purposes," the court said. "And, the FCC's [Declaratory Ruling] and 2015 Order make clear that there is no one way for a caller to obtain consent, and that such consent can be conveyed by another party."

Considering the context of the consent provided by both Baisden and Sissoko, the panel found both forms satisfied the TCPA.

Sissoko's authorization form was nearly identical to that in *Mais*, the court noted, and it "could not be clearer ... as to what Sissoko permitted Mount Carmel Hospital to do with her 'health information'—Mount Carmel Hospital could give it to Consultant Anesthesiologists for the purposes of debt collection, and Consultant Anesthesiologists could give the same to Credit Adjustments."

Further, the plaintiff's cellphone number was included within the scope of "health information," the panel found, concluding that a ruling it excluded would yield a nonsensical result. "[T]he authorization is a contract related to giving consent for medical care, and, as such, 'health information' must be read

through this prism to give it a proper meaning," the court said. "Contact information most undoubtedly is any information that relates to a patient's payment for care provided."

As for Baisden, his authorization form allowed Mount Carmel to use his health information "for as many reasons as needed" and the court reiterated that contact information was included in the scope of "health information."

**"[T]he context in which Baisden and Sissoko provided their cell phone numbers is essential to determining whether they provided 'prior express consent' to receive calls to those numbers," the panel concluded. "They sought medical treatment from Mount Carmel Hospital, and in the course of this relationship, both gave Mount Carmel Hospital their cell phone numbers and authorized it to disclose their cell phone numbers to others. The 'other' in this case—Consultant Anesthesiologists—has a significant relationship to Mount Carmel Hospital, plaintiffs, and most critically, the debts owed by plaintiffs that arose from the transactions in which plaintiffs provided their cell phone numbers. This case, therefore, fits comfortably within the 'prior express consent' limits set forth by the FCC."**

To read the opinion in *Baisden v. Credit Adjustments, Inc.*, [click here](#).

**Why it matters:** Context is everything, the Sixth Circuit emphasized in its decision: the plaintiffs provided their cellphone numbers and authorization for the hospital to share them with third parties and the calls made were in direct relation to the services they received at the hospital. The panel joined the Ninth and Eleventh Circuits to recognize that prior express consent in satisfaction of the TCPA can be provided in a number of different ways, including indirectly.

## Limited VoIP Plan = Cellphone For TCPA Purposes, New York Court Rules

March 25, 2016

**Calls with a prerecorded message or made using an automated telephone dialing system to a Voice-over-Internet number with limited minutes should be treated the same as calls to a cellphone under the Telephone Consumer Protection Act, a New York federal court has ruled.**

Reny Rivero sued America's Recovery Solutions alleging violations of the TCPA based on three calls to his phone number, which had a greeting that directed callers not to leave a message unless in an emergency. Representatives from ARS nonetheless left a voicemail message on each occasion, stating their name and requesting that Rivero return the call to the representative.

Proceeding pro se, Rivero sought damages under the TCPA as well as the Fair Debt Collection Practices Act and state law. Although ARS initially appeared in the action and answered the original complaint, its counsel withdrew after the complaint was amended and then failed to respond to the amended complaint. Plaintiff subsequently moved for a default judgment.

U.S. District Court Judge Eric N. Vitaliano granted the motion and referred the matter to Magistrate Judge Lois Bloom to consider the issue of damages.

The court began by noting that the Federal Communications Commission created a limited exemption for calls between debt collectors and consumers with an established business relationship that extends only to calls made to a "residential line," and not a cellphone or other service.

Rivero's VoIP service from Vonage offers him 300 minutes per month, routing calls through his Internet connection to his phone line. Although little guidance exists in the Second Circuit Court of Appeals on the issue of whether a VoIP intermediary connection alters the nature of the receiving telephone under the TCPA, Magistrate Judge Bloom turned to an opinion from the Fourth Circuit involving a plaintiff that subscribed to a VoIP service that charged her a set amount per call.

In that case, *Lynn v. Monarch Recovery Management*, the federal appellate panel held that because the plaintiff was charged for each of the defendant's calls, the calls were made to "a service for which the party is charged for the call," which is prohibited under the TCPA at Section 227(b)(1)(A)(iii). This conclusion aligned with Congress's intent that automated calls not add expense to annoyance, the Fourth Circuit wrote.

"Plaintiff's VoIP service is not an unlimited calls/flat fee plan as the TCPA presumes is generally the case with a traditional residential telephone line," the court said. "Rather, it is 'a service for which the party is charged for the call' described under Section 227(b)(1)(A)(iii), because each call by Defendant depletes Plaintiff's store of limited minutes. There is no regulatory exemption to this provision because the TCPA permits the FCC to create limited exemptions only to the prohibition of calls to certain cell phones (under subsection (A)) and to residential lines (under subsection (B)). Accordingly, Defendant's calls to Plaintiff's VoIP phone line violated the TCPA."

Turning to damages, Magistrate Judge Bloom denied Rivero's request to treble his statutory damages for the calls and instead recommended he receive just \$500 per call. "Had Plaintiff used a traditional residential line, Defendant's calls would have fallen within the established business exemption and would not have violated the TCPA," the court said. "Given the lack of evidence that Defendant knew Plaintiff would be charged for its calls, treble damages are inappropriate."

The court added \$750 to Rivero's damages for FDCPA violations (with another \$423.50 for costs) but held he could not recover on his New York consumer protection law claim, for a total of \$2,673.50.

Reviewing the report and recommendation, Judge Vitaliano found it "to be correct, well-reasoned, and free of any clear error," and adopted it in its entirety with an order to close the case.

To read the report and recommendation in *Rivero v. America's Recovery Solutions*, [click here](#).

To read the order, [click here](#).

**Why it matters:** The *Rivero* case provides companies that place unsolicited calls to consumers with something new to think about before dialing, specifically, what kind of phone service does the consumer have. Although the defendant elected not to mount a defense in the case, the court found the VoIP plan subscribed to by the plaintiff was "a service for which the party is charged for the call" under Section 227(b)(1)(A)(iii) of the TCPA, triggering liability on the part of the defendant. The magistrate judge declined to treble the plaintiff's damages, however, recognizing that the defendant had no way of knowing that Rivero subscribed to a VoIP plan – had he used a traditional residential line, the calls would have fallen within the established business exemption in the statute and would not have violated the TCPA. A

different outcome might also have been possible had Rivero's Vonage plan featured unlimited minutes. Each call from the defendant reduced the plaintiff's 300 minutes per month, the court explained, leaving room for a defendant to distinguish a situation where a VoIP subscriber had no limit on his calls and would not have been charged for them.

## Tech Company Settles With FTC Over Installation of Apps Without Permission

March 10, 2016

**A technology company that allegedly replaced a Web browser game with a program that installed apps on mobile devices without permission has settled charges that it violated the Federal Trade Commission Act.**

Vulcun purchased Running Fred, a Google Chrome browser extension game used by more than 200,000 consumers. According to the FTC's complaint, the technology company then replaced the game with its own extension, Weekly Android Apps, without notifying consumers. The Vulcun app claimed to offer unbiased recommendations of Android applications, but actually installed apps directly without consumer permission—or as Jessica Rich, the agency's Director of Consumer Protection said in a statement, "commandeer[ed] people's computers and bombard[ed] them with ads."

Google received "a number" of consumer complaints about the Vulcun app, the FTC alleged, not just about the installation of apps without permission, but also that the extension opened multiple tabs and windows on the browser that advertised various other applications and reset users' browser homepages. Consumers also griped that even when they deleted the unwanted apps, Vulcun reinstalled them.

These actions violated the Section 5 prohibition on unfair practices in the FTC Act, the agency alleged in its complaint. "By bypassing the permissions process in the Android operating system, the apps placed on consumers' mobile devices also could have easily accessed users' address books, photos, location, and device identifiers," the agency said. "Indeed, once installed, the apps could have gained further access to even more sensitive data by using their own malicious code."

Vulcun further misled consumers by claiming its extensions provided "independent and impartial" reviews of apps and also it misrepresented the extent of third-party endorsements and media coverage, the FTC added. The company claimed that its app had 200,000 users and a 4.5 rating—a claim that was true for Running Fred, but not for the Weekly Android Apps, according to the agency.

Under the terms of the settlement, the company and two individual defendants must inform consumers about how the information accessed by a product or service will be used, and must also obtain express affirmative consent for the installation or material change of a product or service. Any built-in permissions notices associated with the product must be displayed prior to consent.

Several types of misrepresentations are banned by the proposed consent order. Vulcan cannot mislead consumers as to how personal information is collected and used or how much control they can exercise over the collection, use, and sharing of their data. It cannot misrepresent that a product has been endorsed by a third party or the efforts Vulcan has made to maintain privacy and security of the information collected from consumers.

To read the complaint and proposed consent order in *In the Matter of General Workings, Inc.*, [click here](#).

**Why it matters:** The case offers several lessons for advertisers, the FTC noted in a blog post. It reminds marketers to clearly disclose material information before consumers download a product and to obtain express consent prior to download. In addition, even after a product or service is on a consumer device, companies must stay within the confines of the activities that were disclosed to consumers. Finally, the agency emphasized the importance of disclosures to consumers, particularly where a material connection exists between a product and an endorser. The proposed consent order is currently open for public comment.

## FCC Confirms Different TCPA Liability Analysis for Text, Fax Broadcasters

February 23, 2016

**Denying a petition filed by Club Texting, Inc., the Federal Communications Commission said it will keep its current liability analysis under the Telephone Consumer Protection Act, which separates text broadcasting from fax broadcasting.**

Regulations promulgated by the FCC provide that a fax broadcaster will be liable as the "sender" of an unlawful fax under the TCPA only "if it demonstrates a high degree of involvement in, or actual notice of, the unlawful activity and fails to take steps to prevent such facsimile transmission."

Club Texting, Inc., provides a software platform for companies to contact a target audience via text message. In 2009 the company filed a petition with the FCC for a declaratory ruling asking the Commission to clarify that text broadcasters like itself should be treated consistently with fax broadcasters with regard to liability under the TCPA.

Aside from the technological characteristics of the medium, companies like Club Texting are identical to fax broadcasters, the petitioner argued, and liability should attach only if a text broadcaster "demonstrates a high degree of involvement in, or actual notice of, the unlawful activity and fails to take steps to prevent such transactions."

Clarifying the liability standard would promote compliance, the company added, because its clients are in the best position to ensure that recipients have consented to receive the text messages.

The Commission requested public comment on the issues and received six responses, the majority of which opposed granting the requested declaratory ruling, the FCC said. Concerns were raised about the difficulty identifying the third-party clients of text broadcasters, as well as the fact that the TCPA does not mandate an opt-out notice or sender identification on autodialed text messages. Commenters contended that if the text broadcaster cannot be held liable, then wireless consumers could be left without the ability to enforce the TCPA requirements against any responsible party.

While the petition was still pending, however, the FCC issued its long-awaited omnibus Declaratory Ruling and Order last July, addressing several issues under the TCPA, including liability for text broadcasters.

"Specifically, a 'direct connection between a person or entity and the making of a call' can include 'tak[ing] the steps necessary to physically place a telephone call.' It also can include being 'so involved in the placing of a specific telephone call' as to be deemed to have initiated it," the Commission wrote in the July order. "Thus, we look to the totality of the facts and circumstances surrounding the placing of a particular call to determine: 1) who took the steps necessary to physically place the call; and 2) whether another person or entity was so involved in placing the call as to be deemed to have initiated it, considering the goals and purposes of the TCPA. ... Similarly, whether a person who offers a calling platform service for the use of others has knowingly allowed its client(s) to use that platform for unlawful purposes may also be a factor in determining whether the platform provider is so involved in placing the calls as to be deemed to have initiated them."

The omnibus order settled the issue, the FCC wrote. "[T]he Commission has concluded that the determination as to who is liable as the person who 'makes' or 'initiates' a particular robocall (including an autoialed text message) requires a fact-based determination governed by factors such as which party takes the 'steps necessary to physically place' that call and the extent and nature of involvement by others, including the provider of the calling platform used to make the call," the FCC explained.

Confirming that the July order is the applicable standard for determining text broadcaster liability for TCPA violations, the FCC denied Club Texting's petition.

To read the FCC's order, click [here](#).

**Why it matters:** The Commission has made clear that text broadcasters are subject to a different standard of liability than fax broadcasters under the TCPA, and that the totality of facts analysis adopted in the FCC's July 2015 Declaratory Ruling and Order will be the standard used to determine a text broadcaster's involvement in and potential liability for a wrongful text campaign. The denial of Club Texting's petition did not elaborate on the text broadcasting standard beyond the July 2015 order or provide any additional guidance to businesses.

## Ninth Circuit Affirms TCPA Dismissal Based on Express Consent

February 23, 2016

**The Ninth Circuit Court of Appeals affirmed dismissal of a Telephone Consumer Protection Act class action, agreeing with a California federal court judge that the defendant could not be liable under the statute because the plaintiff provided express consent to be contacted.**

Shaya Baird booked flights online for herself and her family on the Hawaiian Airlines website. During the process, Baird was presented with spaces to enter a number for a mobile phone, home phone, or work phone with the statement, "At least one phone number is required." Baird entered her cell phone number.

Three weeks later and about one month before her departure, Baird received a text message from Sabre, Inc., a travel technology company that contracted with Hawaiian, offering to provide flight notification services if she replied "yes." Baird's response to the text: a putative class action complaint filed in California federal court alleging that Sabre violated the TCPA by sending her an unsolicited text message.

Sabre moved for summary judgment. The defendant argued that Baird consented to receive the text message by voluntarily providing her cell phone number during the online reservation process, even though the number was provided to Hawaiian Airlines and not to Sabre.

The district court agreed and Baird appealed to the Ninth Circuit.

Affirming summary judgment in favor of the defendant, the court relied upon the Federal Communications Commission's 1992 Order prescribing regulations for the TCPA. The agency determined that "persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary."

With the validity of the FCC's interpretation of "prior express consent" not at issue, the Ninth Circuit said the 1992 Order made the appeal easy.

"Baird expressly consented to the text message in question when she provided Hawaiian Airlines with her cellphone number," the federal appellate panel wrote. "Baird knowingly released her phone number to Hawaiian Airlines while making a flight reservation. She did not provide any 'instructions to the contrary' indicating that she did not 'wish[] to be reached' at that number. Therefore, according to the 1992 Order, Baird provided 'prior express consent' to receive the text message in question."

The court also distinguished *Satterfield v. Simon & Schuster, Inc.*, where a panel of the Ninth Circuit concluded that a person's consent to receive calls from one business does not constitute consent to receive calls from a different business. Although a similar situation existed in the *Sabre* case—Baird provided her phone number to Hawaiian Airlines, but was contacted by Sabre—a key difference existed.

"Sabre is a vendor for Hawaiian Airlines and contacted Baird regarding her reservation," the court wrote in a footnote, and the record in *Satterfield* revealed no direct contractual relationship between the entity that contacted the plaintiff and Simon & Schuster. "The district court made no distinction between Sabre and Hawaiian Airlines because of the relationship between the companies, and Baird does not make any argument based on this distinction."

To read the memorandum in *Baird v. Sabre, Inc.*, [click here](#).

**Why it matters:** The Ninth Circuit affirmed the district court's commonsense approach to providing consent and recognized that as a vendor of Hawaiian Airlines, Sabre was able to rely on the consent provided to the airline as prior express consent for the calls it made in connection with the plaintiff's flight.

## Court Certifies Class Against Yahoo! for Welcome Message

January 19, 2016

**An Illinois federal court judge has allowed a Telephone Consumer Protection Act class action against Yahoo! to move forward, certifying a class of roughly half a million plaintiffs.**

Rachel Johnson and Zenaida Calderin alleged they received two messages from Yahoo!'s Messenger feature, which converts instant messages from Yahoo! users into text messages. The first message came from the Yahoo! user and was not at issue. The second, a "Welcome Message" from the company explaining the Messenger service, was unwanted and unlawful in violation of the TCPA, the plaintiffs



claimed. The message stated: "A Yahoo! user has sent you a message. Reply to that SMS to respond. Reply INFO to this SMS for help or go to yahoo.it/imsms."

Johnson and Calderin moved to certify a class of recipients that received the Welcome Message during the month of March 2013 while their mobile numbers were assigned to carriers Sprint and T-Mobile, respectively. Yahoo! objected.

U.S. District Court Judge Manish S. Shah rejected one of the potential class representatives but granted the certification motion with respect to a second, moving the suit forward.

The court found the proposed class was ascertainable and met the requirements of numerosity and commonality, with more than 500,000 potential class members featuring common questions. Turning to typicality and adequacy, Judge Shah agreed with Yahoo! that Calderin was an atypical and inadequate representative because her claim was subject to the defense of prior consent.

Why? In March 2012, Calderin consented to receive the Welcome Message when she agreed to the defendant's universal terms of service, which included contact via text messages. Although she argued that the consent provision did not specifically state such contact might occur using an automatic telephone dialing system, the court found explicit notice for use of an ATDS was "the minority view."

The majority of courts rely on declaratory rulings from the Federal Communications Commission "holding that a person can give express consent simply by providing her cell phone number to another," Judge Shah wrote. "Since the act of giving one's number does not also include communicating permissible or impermissible modes of communication with the giver—yet such an act still constitutes prior express consent—it stands to reason that the TCPA does not require a consentor to specify that an automatic telephone dialing system may be used."

Because Calderin agreed to the terms of service, Yahoo! did not violate the TCPA when it sent her the Welcome Message, the court held.

Yahoo! was not as lucky with regard to Johnson, trying to convince the court she provided consent through an intermediary when she agreed to receive phone calls and texts by filling out an application for a third-party app, which sent her the text via Messenger. Yahoo! was unable to demonstrate that the app provider conveyed consent, the court said, and "[w]ith no such proof, there is no basis to conclude that Johnson or any other recipient gave effective consent through an intermediary."

Judge Shah also found that the requirements for Federal Rule's of Civil Procedure Rule 23(b)(3) were satisfied by Johnson. Individual issues of consent did not overwhelm the common issues with regard to predominance, the court said, as Yahoo! failed to provide evidence to support its theory that intermediate consent or revocation of consent were likely to be significant issues.

The court also held that the class action format was superior to other forms of adjudicating the controversy, rejecting Yahoo!'s argument that certifying a class of plaintiffs for a one-month period with cell phone numbers assigned to a single mobile carrier amounted to piecemeal litigation. "As plaintiffs see it, obtaining a remedy for one month's worth of class members is superior to obtaining it for no months' worth," the court wrote. "I agree."

"I find class treatment to be the superior way to proceed in this case," Judge Shah concluded. "Defendant's concerns are not unreasonable, and there is a prospect that significant management difficulties could arise as the case moves forward. If plaintiff and her counsel cannot provide a manageable, cost-effective plan for identifying and communicating with the class, and resolving issues of consent, then decertification may follow. But without more concrete evidentiary support, defendant's fears are not sufficient to defeat class certification."

To read the order in *Johnson v. Yahoo! Inc.*, [click here](#).

**Why it matters:** While Yahoo! was able to remove one potential class representative from the suit, the court found the second representative met the necessary requirements to certify a class that could yield half a million members. To make matters worse for Yahoo!, it faces similar suits in other courts, including California, though the judge in that litigation reached the opposite conclusion [last year](#), denying the plaintiff's certification motion after finding that the class was not ascertainable.

## NOTES

# Index

## A

Advertising Law Newsletter  
mobile marketing, [455–469](#)  
native advertising, [435–448](#)  
social media, [449–454](#)

## B

Big Data  
seizing opportunities, preserving values, [323–333](#)  
tool for inclusion or exclusion  
appendix, Commissioner  
Maureen K. Ohlhausen,  
separate statement, [417–418](#)  
big data's benefits and risks,  
[387–394](#)  
conclusion, [415](#)  
considerations for companies in  
using big data, [394–414](#)  
executive summary, [377–381](#)  
introduction, [383–385](#)  
life cycle of big data, [385–387](#)  
Big Data and Privacy  
Presidents' Council of advisors on  
science and technology  
collection, analytics, and  
supporting infrastructure,  
[279–292](#)  
examples and scenarios, [271–278](#)  
executive summary, [255–260](#)  
introduction, [261–269](#)  
PCAST perspectives and  
conclusions, [307–313](#)  
technologies and strategies for  
privacy protection, [293–305](#)

## C

Cloud Computing, SaaS and Outsourcing  
benefits and risks, [118–119](#)  
contract issues, [120–121](#)  
overview, [117–118](#)  
vendor or the customer, laws and  
standards, [120](#)

23rd Computers Freedom and Privacy  
Conference  
Julie Brill, keynote address,  
[337–348](#)

## D

Digital Advertising Alliance  
transparency and control to data  
used across devices  
control, [358](#)  
overview, [355–356](#)  
transparency, [357](#)

## E

Emerging, Disruptive and Sharing  
Technologies  
sharing economy  
case study, [63–64](#)  
current legal issues,  
[64–69](#)  
definition, [55–58](#)  
going, where, [61–63](#)  
origin, [59–61](#)  
take aways, [70](#)

## F

Faculty Bios  
Alison Pepper, [46](#)  
Bonnie L. Yeomans, [52](#)  
Christin McMeley, [41](#)  
Esra Hudson, [36](#)  
Jim Snell, [27](#)  
John C. Yates, [51](#)  
Joseph J. Lazzarotti, [38](#)  
Joseph V. DeMarco, [34](#)  
Keith Larney, [37](#)  
Keith Yandell, [50](#)  
Laura D. Berger, [29](#)  
Lucian T. Pera, [47](#)  
Marc Roth, [26](#)  
Marty Collins, [33](#)  
Michele C. Lee, [39](#)

## Faculty Bios (*Cont'd*)

Michelle Perez, [48](#)  
Noga Rosenthal, [49](#)  
Pamela A. Bresnahan, [30](#)  
Philip L. Blum, [25](#)  
Robert H. Cohen, [31–32](#)  
Scott Maples, [40](#)  
Tristan Ostrowski, [45](#)  
Tsan Abrahamson, [28](#)  
Tyler Newby, [42–44](#)  
William H. Efron, [35](#)

FTC Warns Marketers That Mobile Apps  
May Violate Fair Credit Reporting Act  
agency sends letter to marketers of  
six apps for background  
screening, [365–366](#)

## I

*In re Apple v. FBI*  
amicus curiae, [147](#), [151–152](#)  
conclusion, [164–165](#)  
facts and summary of argument,  
[153–164](#)

## P

Program Schedule  
cloud computing, SaaS, and  
outsourcing, [12](#)  
cybersecurity, hacking, and data  
breach, [13](#)  
emerging issues in big data and  
analytics, [15](#)  
emerging, disruptive, and sharing  
technologies, [11](#)  
evolving legal ethics: portable  
devices, the cloud, and social  
media, [14](#)  
hot topics in tech law litigation, [13](#)  
the internet of things and the wired  
life, [15](#)  
reaching consumers in a digital  
world: marketing, advertising,  
and social media, [16](#)  
the virtual workplace, [11](#)

## S

Summary of 2016 Internet of Things Cases  
cases  
automobiles, [229–231](#)  
consumer electronics, [232–236](#)  
medical devices, [231–232](#)  
smartphone applications,  
[227–229](#)  
world-wide web outage, [236](#)  
introduction, [227](#)

## T

Tech Law Litigation  
challenges to article III standing,  
[127–128](#)  
choice of law provisions in terms of  
service, [136–137](#)  
class certification developments,  
[137–139](#)  
international discovery  
developments, [140–142](#)  
online agreements & arbitration  
provisions, enforcement,  
[129–135](#)  
patent litigation trends, [139–140](#)

## U

*U.S. v. Knowles*  
complaint, [169](#)  
consent preliminary order of  
forfeiture as to specific  
property/money judgment,  
[169–194](#)  
letter in response to order of the  
court, [195](#)  
order, [197](#)  
Use of Cloud Computing, Mobile Devices  
and Social Media in the Practice of  
Law  
conclusion, [215](#)  
hypotheticals, [216–220](#)  
managing ethical risks,  
[201–206](#)

social media, [209–214](#)  
using mobile devices, [206–208](#)

## V

### Virtual Workplace

BYOD risks and remote access,

[75–77](#)

California’s definition of

“reasonable safeguards” for

protecting personal data, [100–103](#)

controlling employee data security

risks, [103–112](#)

employee monitoring,

[81–100](#)

using social media,

[77–81](#)

## W

### WP29 on the Impact of the Development of Big Data

protection of individuals with regard

to the processing of their

personal data in the EU,

[427–428](#)

