INTELLECTUAL PROPERTY
Course Handbook Series
Number G-1277

Seventeenth Annual Institute on Privacy and Data Security Law

Volume Two

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

To order this book, call (800) 260-4PLI or fax us at (800) 321-0093. Ask our Customer Service Department for PLI Order Number 148906, Dept. BAV5.

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

53

Top 10 Privacy and Cybersecurity Issues in M&A (May 16–17, 2016)

Sue Gomez
ScanDisk Corporation

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

INTRODUCTION

Compliance with privacy laws and cybersecurity regulations is an essential consideration in merger and acquisition (M&A) transactions. Wise dealmakers consider data privacy and security when establishing the appropriate valuation of the M&A target, particularly when large databases containing consumer, health and financial data is involved. Failure of the target to meet its privacy and data security obligations (under law or its own policies and representations) can present a significant risk to the acquirer. Penetration incidents, such as point of sale attacks, phishing and ransomware, may require significant resources to investigate, defend and mitigate and remediate. Boards and deal teams need to be aware of risk derivative actions, successor private rights of action, regulatory scrutiny and fines. This article sets forth some considerations for counsel in the pre-acquisition due diligence and post-deal phases of the M&A transaction.

CHECKLIST SUMMARY: TOP 10 PRIVACY AND CYBER SECURITY ISSUES IN M&A

#1: Due Diligence will be grueling

#2: Privacy may be just as important as the IP

#3 Cybersecurity permeates all aspects of the deal

#4: Convergence of privacy and competition law may trip you up

#5: What the target hasn't done can be just as damaging as what they have

#6: Target's third party diligence program will prove important

#7: Governance *is* a differentiator – board minutes, training records and audits are golden

#8: When it comes to personal information, the acquiring company's intentions matter

#9: Reputation and trust forms the basis for all things privacy

#10: Bad things can and do happen to good companies – be upfront about what happened and what was learned

CHECKLIST

#1: Due Diligence will be grueling

M&A activity continues to flourish with mega-deals leading the charge. Privately-held company acquisitions in the technology, media and data analytics space are growing as well. Dealmakers need to establish the proper valuation of the M&A target. Lax privacy internal processes and controls raise flags when data plays a significant part of the transaction and the deal's valuation. This means that in addition to employee data privacy and deal security considerations, the customer lists, databases, data mining tools, analytics, and research technologies are important too. Failure to pay heed to these during due diligence could render a key database unavailable or incompatible with the acquirer's plans. Mismanaged financial or health data could render the data a liability rather than an asset. As appetites for deals grow, a methodical due diligence privacy framework is recommended prior to inking the deal. Some key elements are listed below.

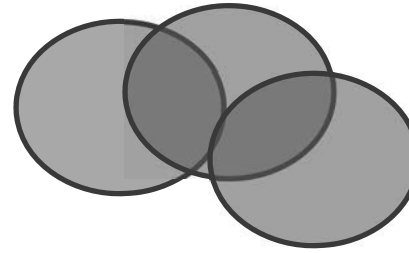
1. Identify the target's data sets, classification, sensitivity levels
2. Identify acquiring company's planned uses for the target's data
3. Assess risk based on valuation method
    a. Market compares, present value calculations, venture valuation
4. Is the data of known pedigree, segregated and easily isolated?
5. Is there duplication with acquiring company's existing data?
6. Identify key privacy risks
    a. Privacy promises
        i. URLs, posted information, opt-ins, other representations, last update
    b. Privacy Notices, sector-based Requirements (financial, health care, children)
    c. Customer support, forums, portals, online profiles
    d. E-commerce, terms of service
    e. Worker data policies, consents
    f. Cross-border transfers
    g. Data localization

h. Foreign accessibility, attributions

7. Identify the target's marketing practices
    a. Email marketing, Opt-in, CAN-SPAM Act compliance
    b. Telephone or Text Messaging? Telephone Consumer Protection Act (TCPA)
    c. Online behavioral advertising (OBA)
    d. Tracking, cookies, flash cookies, web beacons (placed for OBA or other purpose (strictly necessary, analytics); do not track/DNT)
        i. First party or third party
    e. Ad networks
        i. Third party ad placements
        ii. Ad retargeting
    f. B2B, B2C, B4B
    g. Social Media site capture, posting
    h. Analytics
8. Identify and review the target's apps and technology
    a. Business model for each product
        i. Purposed tracking
        ii. Data capture, sharing, storage, format, duration
    b. Consent model
    c. Security model
9. Identify worker data approach
    a. Global, regional databases
    b. ERP, SaaS, Hosted Cloud
    c. Tools, Analytics
    d. Cross border access and transfer
    e. Method of legal transfer, consent model
    f. Data protection authority registrations
    g. Policies, consent, employee notice, localization

10. Is the target a regulated entity? Common US bodies include:
    a. Gramm-Leach-Bliley Act (GBLA): Financial Institutions including background checks
    b. Health Insurance Portability & Accountability Act (HIPAA)/ HITECH Act, business associates
    c. Financial Agency: FACTA, Fair Credit Reporting Act (FCRA)
11. Does target collect Social Security Numbers?
12. Does target operate a website or sell products targeting children under 13? (COPPA)
13. Does target manage transactions accounts (e.g. mobile phone account, savings or checking account, utilities)? Is target subject to the Red Flags Rule?
14. Does target handle medical information and comply with CA Confidentiality of Medical Information Act?
15. Is the target involved with e-commerce, maintain Payment Card Industry (PCI) standards?
16. Do specific federal and state laws apply to the collection, use, disclosure of:
    i. Protected Health Information (HITECH)
    ii. Educational data (FINRA)
    iii. Credit data (FCRA)
17. Security
    a. Ask about target's data security incidents, any actions by state or local authorities, fines by Payment Card Industry or other standards groups, private or class actions, settlements, consent decrees, identifiable customer losses due to privacy or security controls, investigations or notice of investigation by an authority or regulator around the world.
    b. Ask to see the target's incident response program.
    c. What controls, encryption or otherwise, protect the current data from disclosure or breach?
    d. Does the company maintain a data breach "tiger team"?

18. Products
    a. What current products or services collect data, how are they managed, where is the data stored?
    b. What products or services are planned or under development?
    c. What is the "privacy by design" due diligence approach? Does the company perform privacy impact assessments?
19. Advertising/Web Tracking
    a. Ask about the target's social media strategy
    b. Does the company allow first and third party cookies, for what purpose? What analytics are performed? What disclosures are made in compliance with EU Cookie Directive, CalOPPA and Do Not Track? Does the target company comply with right to be forgotten requests? How?
    c. If target is a data mining company, what tracking technologies are used? What is their strategy for de-identification?
    d. Does target rely on ad agencies and digital marketing activities? Are these properly disclosed?
20. Global Databases
    a. What is the target company's strategy for global HR transactions? Where are databases housed; and from where are they accessed, and by whom?
    b. How does the company comply with cross-border transfer rules?
    c. Does the company maintain data flows and privacy impact assessments?



#2: Cybersecurity permeates all

Unfortunately cybercrime, cyber-ransom and data breach are all too commonplace. When personal data is collected and stored by the target, the acquirer will absorb the liability and obligations post-close.

Having a robust data privacy and security program which limits collection and use for the purposes collected, limited retention, and destruction help to ensure the acquiring company is not buying a lawsuit or worse yet, a public relations nightmare.

Privacy depends on security

Security without privacy is possible, privacy without security is not

Consider the following:

1. Does target deploy encryption technologies? When, where, what circumstances (e.g. in transit, at rest)?
2. Does target have record retention policies, data classification?
3. Who has responsibility for physical, technical and administrative controls?
4. What is the target's data loss prevention strategy?
    a. Does the target require and offer secure data disposal?
    b. Does the target allow Bring Your Own Device, work from home, flash drives?
5. Does target maintain an incident response plan?
6. Has the target experienced one or more data breaches? Obtain copies.
    a. What was the root cause, the scope
    b. What fines or other consequences resulted
        i. Action of State AG, FTC, authorities
        ii. PCI fines
        iii. Class actions
        iv. Regulator letters, cease and desist
        v. Customer notice, credit monitoring, dissatisfaction, defection
    c. What lessons were learned, mitigations deployed
7. Does target allow personal information about consumers or workers to reside on laptops, mobile devices
    a. Describe security, encryption policies
8. Are the target's employees trained on how to spot spamming, phishing, cyberattacks

9. Has any adverse media or publicity experienced by the target for cyber matters

10. Ask about target's data security incidents, any actions by state or local authorities, fines by Payment Card Industry or other standards groups, private or class actions, settlements, consent decrees, identifiable customer losses due to privacy or security controls, investigations or notice of investigation by an authority or regulator around the world.

    a. Ask to see the target's incident response program

    b. What controls exist to protect the current data from disclosure or breach?

    c. Does the company maintain a security breach "tiger team"?

    d. If selling products - what is the current security profile for current products or services that collect data, how are they managed, where is the data stored?

    e. What products or services are planned or under development? What is the "security by design" due diligence approach?

#3: Privacy can be just as important to valuation as IP

Data is the "lingua franca" and currency of sorts in many business deals. The hunger for more "eyeballs," consumer intelligence, data mining, data analytics, and predictive coding means soaring valuations for web properties that collect, analyze and sell data. It also means that for the buyer, data integrity and data pedigree is as important as traditional intellectual property. As a result privacy should be on every due diligence checklist for review in the data room. Without proper consent, history, expectation of legal acquisition, the data so highly coveted may be worthless. Here are some considerations.

During Early M&A Discussions:

1. Value data realistically, consider duplications, review sample databases with skeptical eye, was it organically collected or bought from an agent, reputable? Is it scalable or one time? Does it have a long "shelf life" (stable users) or is it fleeting?

2. Is it really usable, in an available format, without encumbrances to the target?

    a. Ask could the target delete or vault this data with no one else laying claim to it

3. Are consents broad enough to cover expected new uses of the acquiring company?
4. Will customers pull their consents or fail to opt-in once notified of the merger?
5. Will data protection authorities need to be notified?
6. Will the bloggers erupt in contempt or joy?
7. Does other parties have claim to the compilations? Is there an expiration date?
8. Is there a purpose limitation that could be "challenged" or can't be re-purified via post-close opt in?
9. Does the privacy policy of the target allow for transfer of personal data to the acquirer? If so, at what stage of transaction?

During Due Diligence

1. Check Privacy Statement /Policy and consent promises for disclosure and use obligations
2. Is there a right to assign the data to new owners?
    a. Particularly if reverse triangular merger, check for change of control
    b. Asset sale, new owner
3. What about branding questions, disclosures about who is in control of the data
    a. Day 1, Day 45, Day 90
4. Federal Trade Commission (FTC), Department of Justice (DOJ), Data Protection Authorities (DPA) may want the opportunity to ask questions
5. Check status of Safe Harbor (now defunct expected to be replaced by Privacy Shield), assignability of Standard Model Contracts or Binding Corporate Rules
6. For EU, consider consents given lack of derogations
7. Check validity of "successor and assigns" and need to obtain new and separate valid or specific consents

Post-Merger

1. Notification to customers, what is sufficient?

2. Send out "challenge" renewing opt in?
    i. what is the default
    ii. what is legally sufficient
3. Carefully consider localization and segregation issues
4. Set down unresolvable data, consider an escrow
5. Use care before combining
6. Continue chain of custody, retain file headers/label data as to source and nature of opt-in and purpose

#4: Convergence of Privacy and Competition Law may trip you up

Privacy may be considered a form of non-price competition, like quality of innovation. Consequently, privacy issues may form the basis for an M&A challenge by the US Federal Trade Commission or the Department of Justice if believed to result in a substantial lessening of competition due to higher prices, lower quality or reduced innovation.

FTC

In fulfilling its mission to promote competition and protect consumers, Section 5 of the FTC Act can involve analysis of potential merger related activities that could lessen privacy related competition. FTC opinions in Google Inc. and DoubleClick and other have laid the framework for review if a merger adversely affected non-price attributes of competition in data-rich companies.

U.S. Department of Justice

Companies in mergers and acquisition talks should expect privacy considerations in the antitrust review particularly if there are large databases of consumer information involved. Expect inquiries into to how the data will be used post-merger, how the merger will affect consumer privacy protections, how data will be maintained, protected and used.

Bureau of Competition and Bureau of Consumer Protection

The focus is on whether the transaction could result in decreased privacy protections for the consumers, such as with lower quality of

privacy protections, and whether the combined companies achieve market power as a result of the combination of their data.

International

International investigations tend to focus on whether there is a decrease in privacy competition or the combination of companies would result in a dominant company with less privacy or there is a concern of consumer backlash. In a Privacy and Competiveness in the Age of Big Data (2014) publication, the European Data Protection Supervisor set forth a goal for agencies to assess gaps between EU competition law, consumer protection and data protection policies.

Non-Price Competition Reviews

Be prepared to provide:

a) The target's privacy practices including:
   1. Privacy statements to consumers, changes and updates
   2. Cookie statements
   3. Ad networks, analytics tools, e-commerce

b) Economic analysis of the combined company's competitive impact on the market for data, impact on privacy protections, efficiencies

c) Pre-existing market power concerns/mitigations

d) A tutorial on how the combined company will address consumer data, notice/ choice, storage, opt-outs, text and mobile marketing, storage and data security privacy protections post-transaction

#5: What the target hasn't done can be just as damaging as what they have

If the target deploys public cloud for data collection, processing and storage, the key issues may be whether the due diligence, data location, service commitments and right of access and chain of control are robust enough to give the acquiring company comfort that data breach or misappropriation has not or will not occur. With so many providers saying "take it" or "leave it" with their cloud contracts, many companies will "take it" and hope for the best. With respect to third party contracts, the acquiring company should assess:

1. Transferability
    a. Degree data format is custom to the provider platform
    b. Can the data be transferred in-house or to a more secure provider
2. Data Location and Compliance
    a. Consistency with privacy promises, encryption, reasonable security
    b. Applicable consents, have Data Collection Authorities been properly notified
    c. Localization and data transfer regimes
3. Third Party Service Providers
    a. Whether to continue using the same providers based on terms, service options, existing vendors
4. Products
    a. What current products or services collect data, how are they managed, where is the data stored
    b. What products or services are planned or under development? What is the "privacy by design" due diligence approach? Does the company perform privacy impact assessments?
5. Security
    a. What controls exist, encryption or otherwise, to protect the data from disclosure or breach?
    b. Disaster recovery plan; data backups
6. Social Media Strategy
    a. Does target company have a social media policy e.g. who can speak on behalf of the company, social media and the recent opinions of the National Labor Relations Board (NLRB)?
    b. Ask about use of social for advertising, ad agencies and digital marketing activities? Are links and auto-sharing properly disclosed?
7. Global Databases
    a. What is the target company's strategy for global HR trans-actions?

b. Does the company obtain and maintain specific consents?

c. Are databases housed locally (e.g. Russia)? How does the company comply with cross-border transfer rules (e.g. EU)

d. Does the company map data flows?

e. Does the company perform and maintain privacy impact assessments?

#6: Target's third party diligence program will prove important

The use of third party service providers is ubiquitous and inevitable. Most likely target has some functional data stored with a service provider and chances are it contains personal information, worker or financial data. The FTC generally and EU Cloud Directive specifically mandate adequate protections including breach notification and 47 states in the US have specific laws that prescribe what needs to be done upon notice of or suspicion of breach. The EU General Data Protection Regulation (GDPR) is expected in 2018 to give companies 48 hours to notify authorities and/or data subjects of breach. Privacy officers in conjunction with IT Security and Audit departments can make a significant difference in the due diligence process by having documented records of the security checks, analysis and periodic audit/vendor verifications.

Among the key issues in cloud and service provider contracts are whether the customer will have control and visibility over sub-contracting, the provider's ability to change the nature of the services provided, the privacy and data security commitments and will the provider be able to suspend services under commercial circumstances such as non-payment or violation of a terms of use policy. Other key terms are the rights to termination assistance/migration to an in-house or replacement solution and if force majeure provisions are one-sided capture of all changes including change of laws. General questions to ask:

1. Does the target use multi-tenant cloud services?
2. Does the target know where data resides and have audit rights to verify data integrity and SLAs?
3. Does the target have an information security program sufficient to handle third party risks?

4. Does the target deploy software and penetration testing to ensure data is not compromised?
5. With respect to third party providers and cloud vendors, has target performed pre-onboarding security reviews?
6. Does the target negotiate its contracts for sufficient data security terms, and in line with its own privacy policy commitments?
7. Does the complex contract structure or URL links impede the provisions of a negotiated contract?
8. Do contracts contain sufficient notice of breach, material changes, subpoenas, law enforcement requests, governance, audit rights, service levels, termination assistance, limitation of liability clauses and appropriately limited force majeure clauses?

#7: Privacy/security governance is a differentiator – board minutes, training records and audits are golden

Governance in the form of general risk & controls plan, privacy and data governance programs is often segregated by type of data or risk. For example, privacy governance may exist as part of the worker (HR) function, which is different from marketing and different from IT and Info Security. M&A privacy due diligence often touches on all these areas requiring the chief human resources, privacy and chief information security officers to work together to respond. Targets should be able to produce documents to illustrate the governance models for data they collect, store and maintain. Minutes of executive and board meetings, trainings, and risk assessments can help explain what has been done. Here are some questions to ask:

1. Does the company have internal policies regarding collection, storage, retention and disclosure of personal and sensitive information and the devices that contain such data? Are consents obtained and honored? How does the company use cross-border model clauses, binding corporate rules or now defunct Safe Harbor for cross-border EU transfers? What are they doing in place of Safe Harbor?
2. Does the target's enterprise risk assessment include privacy and data security? Has the Board been briefed on Cybersecurity and Privacy practices? How often?
3. Does the target require periodic training of all employees relative to privacy practices?

4. Are third parties screened and background checks performed where legal and applicable?
5. If in a regulated industry, such as financial, broker-dealers, advertising networks, e-commerce, broker-dealers, healthcare or government, are basic levels of diligence evident in the target's internal processes and controls?
6. Does the target collect personal information from children under 13? Are internal controls and consents required by Children's Online Privacy Act (COPPA) in order?
7. Does the company have/maintain a records retention policy?
8. Does the target have and maintain a written information security program (physical, technical and device level)? Have a robust Incident Response Plan? Run "desktop" exercises to verify its efficacy?
9. Does the target deploy policies around Bring Your Own Devices (BYOD), remote work, use of USB and other external devices for storage? What are policies related to data confidentiality and due diligence for data onboarding or purchase of lists to ensure the company's proper entitled uses are honored?
10. What data loss escalation procedures and policies exist to ensure data doesn't "walk out the door" when someone leaves the company and unauthorized data doesn't "walk in the door" upon onboarding?
11. What audits or risk assessments have been performed? These often contain insights to the areas of risk and mitigations.

#8: When it comes to personal information, the acquiring company's intentions matter

Understanding what the acquiring company intends to do with the target's data is critical to assessing gaps and determining what to make available in the data room. Unfair and deceptive practices (Section 5 of FTC Act) can result when a company promises one thing in their privacy statement or consent notifications but actually practices something very different. Hidden cookies, tracking tools or third party networks may be deployed by the company or its service providers without full disclosure to the consumer, agencies or employees. Overly broad representations and warranties in the stock purchase agreement or due diligence documentation may give false promises about the integrity and robustness of the target's privacy

program. A savvy acquiring company will ask the questions during due diligence because post-acquisition, it will assume responsibility for target's practices and will bear the burden of any litigation, class actions, civil and criminal penalties.

Privacy Promises

- Review the target's privacy statement, contracts with customers, vendors and intercompany agreements to assess limitations on use, transfer and conditions, adequacy of data security and data integrity.
- Identify acquiring company's planned uses for the data, cross-border transfers that may be incompatible with the target's privacy statement promises.
- Assess gaps and plan for Day 1 compliance or "challenge" consent steps to address (segregate or retire) the data.

Web Properties and Social Media

- Which privacy policy will govern on Day 1?
- Segregate collected data until consents and transition is fully performed.
- Ensure data security at all stages.

Products Support

- Notify existing customers of change.
- Explain how their data will be maintained, secured, explain new entity and policies, and allow ample time to consent/opt out.
- If regulated, obtain opt in/consents in writing; non-regulated best practice: assume opt- out until an affirmative opt in.

Employment Context

- Consent is tricky in employment context. Target and acquirer share in solving this.
- Cannot assume that derogations apply "necessary for performance of obligations of a contract to which the data subject is a party, or to comply with specific requests of the data subject" as it relates to employee data in M&A.
- Obtain specific consent and execute standard model clauses between target and acquiring company.

#9: Reputation and trust form the basis for all things privacy

This applies to employees, consumers, and regulators alike. Merited or not, allegations can destroy a program and the value of the acquisition. Senior management has to be responsible for caring about and trickling down a culture of compliance, respect for privacy data integrity and security. With fines/penalties set forth in the General Data Protection Regulation expected to be the greater of $20M euro or 4% annual revenue turnover, the stakes couldn't be higher. Just like Boards that fail to take cybersecurity into their fold do so at their own "peril" (Luis Aguilar, Commissioner SEC in a speech June 10, 2014 to Boards of Directors), regulators will likely not consider exempting or reducing the fines for companies UNLESS they can demonstrate adequate procedures and internal controls to avoid data breaches and meet privacy commitments. Here's what wise dealmakers can do:

1. Assess the character and compliance culture of the target
    a. Read the target's Code of Business Conduct
        i. Does it include privacy and data security?
        ii. Is it respectful of privacy rights and cultures?
        iii. What's the tone from the top?
    b. Do they have a privacy training program? Is it global? Do they place personal accountability front and center in their policies and practices?
    c. Does the target's ethics hotline include privacy and data security? Ask for instances and how they were resolved.

#10: Bad things can and do happen to good companies - be upfront

Information about the target's deficiencies can be found during due diligence but the fact that a breach occurred is not in and of itself a deal killer. Instead how the company handles the actual or suspected breach, the lessons learned and respect they have for the personal and sensitive information rights can give the acquirer much needed information about steps to ask for prior to close. Ask the target company to:

1. Explain its data protection and cybersecurity risk assessment program and mitigations.

2. Describe any claims brought or anticipated against the company by consumers, employees, class action bar, agencies, states attorney generals, data protection authorities, governmental and non-governmental bodies.
3. Provide enough detail for the acquiring company to assess the level of risk and remedial steps to be taken before close or immediately thereafter.

CONCLUSION

In summary, there are numerous reasons and competitive incentives behind mergers and acquisitions, corporate transactions and spin offs. Including privacy rights and reasonable data security program assessments in the transaction due diligence before, during and after the deal helps companies properly handle data assets. Broadly reviewing the target's practices against acquirer's intended uses can help prevent surprises on Day 1 and possible successor liability.

Disclaimer: This segment on Top 10 Privacy and Cyber Security Issues in M&A was prepared for and is intended as general guidance for use in the 2016 PLI Institute on Privacy and Data Security Law Conference, San Francisco, CA. The statements and errors are my own and not those of my company and should not be construed as legal advice or serve to establish an attorney-client relationship.

NOTES