Morgan Lewis

What Every General Counsel Should Know About Privacy and Security: 10 Trends for 2014

Morgan Lewis Webinar

March 18, 2014

Reece Hirsch, CIPP, Partner

Morgan Lewis

Privacy as a Front-Burner Issue

- Much of the law of privacy and security is still relatively new
- Not so long ago, privacy was considered an arcane subject that was primarily the province of IT and security professionals
  - Few companies had privacy officers
- Each year it becomes more and more clear that privacy is a critical legal compliance issue

A Question of Trust

- Failure to appropriately address privacy and security compliance is a bottom-line issue for companies because
  - Privacy is personal
  - Privacy goes right to the heart of a consumer's relationship with a company
  - It is very easy to make mistakes given the complex patchwork of state, federal and international laws
  - Privacy and security regulatory enforcement and litigation are on the rise

1. Mobile App Privacy

- The proliferation of mobile apps poses unique privacy concerns:
  - Collection of enormous volumes of personal information by smartphones and tablets
  - Ability to tie that data to specific individuals through geolocation data
  - Complex ecosystem of players (operating systems, app developers, ad networks)
  - Difficulty in providing robust privacy disclosures on small mobile device screens

FTC Advice on Mobile Privacy

- February 2013: FTC Staff Report "Mobile Privacy Disclosures: Building Trust Through Transparency"
  - Offers suggestions on privacy transparency for mobile platforms and app developers
  - Generally consistent with the California Attorney General's January 2013 privacy recommendations for the mobile ecosystem
  - As in many other areas, CA spurs the national privacy conversation

FTC Advice for Mobile App Developers

- Post a privacy policy and make it available through the platform's app store so consumers can review before downloading
- Provide "just in time" disclosures and obtain affirmative express consent when collecting sensitive information (financial, health or children's data) outside the platform's application programming interface (API)
  - Or when the app shares sensitive information with third parties

FTC Advice for Mobile App Developers (cont.)

- Improve coordination and communication with third parties that provide services for the apps (ad networks, analytics companies) so that app developers can more accurately disclose their data collection practices to users
- Participate in self-regulatory programs, trade and industry organizations that may develop guidance on uniform, short-form privacy disclosures
  - July 2013: Draft Voluntary Code of Conduct for mobile apps arising from Dept. of Commerce's National Telecommunications and Information Administration stakeholder meetings

Federal Mobile App Privacy Enforcement

- February 2013: FTC settles with Path, Inc., a social network service that allows users to share journals with friends in their network
- FTC alleged that Path *automatically* collected and stored personal info from the user's address book even if user did not select "find friends from your contacts" option
- $800,000 fine (based on legal authority under the Children's Online Privacy Protection Act (COPPA))
- Mandated privacy compliance program and required independent assessments every other year for 20 years

California Mobile App Privacy Enforcement

- October 2012: California Attorney General issues warning letters to companies for failure to post mobile app privacy policies
  - Citing authority under the California Online Privacy Protection Act (CalOPPA)
  - AG views CalOPPA as applicable to operators of online services that collect personal information of CA residents
  - CalOPPA requires crafting a compliant privacy policy and posting it “conspicuously”

2. Data Security Compliance Programs

- Privacy has long been a subject of state and federal legislation, but data security laws are a relatively recent development
- It is becoming increasingly clear that development of a formal, written data security compliance programs is a best practice
- Under a patchwork of state and federal laws, they are also often required
- Data security has been the most cited issue for GCs and directors for past 2 years in a survey by FTI Consulting and Corporate Board Member

“Proactive” Data Security Laws

- The HIPAA Security Rule
  - Now applicable to business associates pursuant to the HITECH Act
- Gramm-Leach-Bliley “safeguards” regulations
- State insurance privacy law “safeguards” measures
- General state security mandates in Massachusetts, Nevada, California, Connecticut, Rhode Island, Oregon and Maryland

“Reactive” Security Breach Notification Laws

- Part of trend that started in 2005 after ChoicePoint incident
- 46 states (plus D.C., Puerto Rico and Virgin Islands) have security breach notification laws
- Many of the laws incentivize use of encryption by providing that notification is not required for a breach involving encrypted data
- HITECH Act sets rigorous new breach notification standards that expand upon state law measures, but limited to HIPAA covered entities, business associates and personal health record (PHR) vendors and related entities

The FTC's Unfairness Doctrine

- In 2005, the FTC articulated the "unfairness doctrine" in the settlement of an enforcement action involving BJ's Wholesale Club
- Previously, FTC had based its data security enforcement efforts on its authority to regulate "deceptive," rather than "unfair" acts or practices
  - If a company said nothing about its information security practices, then FTC had no jurisdiction

The FTC's Unfairness Doctrine

- The FTC only needs to show that a company's information security practices:
  - Cause or are likely to cause substantial injury to consumers
  - That the harm to consumers is not reasonably avoidable by consumers themselves
  - That the harm is not outweighed by countervailing benefits to consumers or to competition

Is the Unfairness Doctrine Unfair?

- *FTC v. Wyndham Worldwide Corp. (U.S. Dist. Crt., NJ)*
  - November 2013: Oral arguments on Wyndham's motion to dismiss arguing that FTC lacks authority under Section 5(a) of the FTC Act to establish and enforce data security standards
  - Wyndham maintains that the unfairness prong has traditionally been read to prohibit unconscionable acts toward consumers
    - *Does not provide justification for taking on the new policy area of data security*
  - A case to watch, along with the FTC's LabMD action

Recommended Steps

- As part of overall oversight of risk management, a CEO should report regularly to the board on the company's security risk profile and related internal information governance systems
- Companies should develop a security strategy under the direct supervision of a C-level officer
  - Strategy should be documented in a written security compliance program
- Companies should consider how their trade secret and IP could be better protected in light of domestic and foreign cyber threats

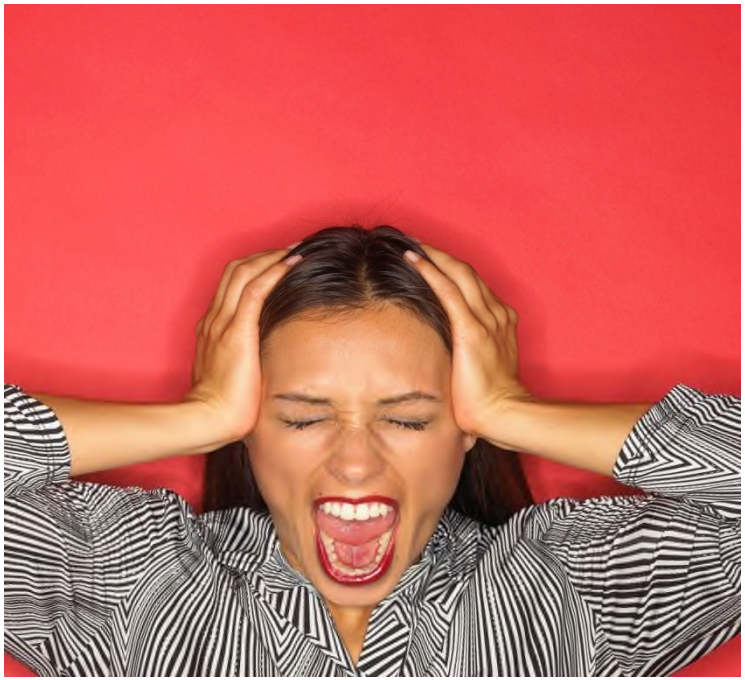
3. Security Breach Response

- The drumbeat of major security breaches continues
- Cybercriminals are increasingly sophisticated, targeting large databases of customer information.
  - Often seeing export of data to URLs in China, Russia
  - Corporate trade secrets and IP are increasingly a target
- Review of Major 2013 security breaches

Have We Reached the Tipping Point?

- January 2014: Personal Data Privacy and Security Act of 2014 introduced by Sen. Leahy
  - Would create a national standard for data breach notification and require adequate security practices
  - May finally gain traction this time

The Dreaded Security Breach



The Worst Case Scenario

- Most security breaches are garden-variety incidents that do not pose significant risks if properly handled
- A major security breach that results in actual damages can lead to:
  - Class action lawsuits
  - Drop in stock price for public companies
  - Regulatory action by state Attorneys General or other regulators
  - DAMAGE TO BRAND AND CUSTOMER RELATIONSHIPS

Common Security Breach Response Mistakes

- Understand whether you are legally obligated to notify affected individuals
  - Don't overreact
  - Can't "unring the bell" once a notification letter has been sent
- Remember that the triggers for notification under state laws differ.
  - Is there a "reasonable belief" that the information has been acquired by an unauthorized person (California)?
  - Is there a "likelihood of harm" (Delaware)?

Common Security Breach Response Mistakes

- In a notification letter, address the risks posed by the particular breach
  - If the breach involves medical information, address the risk of medical identity theft and how to mitigate
  - If the breach involves Social Security numbers or financial account information, address risks of financial fraud and identity theft

Common Security Breach Response Mistakes

- Failure to train your workforce to spot and report a security breach immediately
- Failure to require prompt security breach notification in agreements with vendors/agents
- Failure to organize your incident response team in advance
- In a recent FTI Consulting survey, 27% of directors said their company did not have a written security breach response plan; 31% weren't sure

Incident Response Plans

- An effective incident response plan should:
  - Establish an incident response team with representatives from key areas of the organization (Compliance, Legal, HR, PR, investor relations, IT, etc.)
  - Identify necessary external resources in advance (forensic IT consultant, mailing vendor, call center operator, credit monitoring service)
  - Provide for training of rank-and-file personnel to recognize and report security breaches
  - Outline media relations strategy and point person

Breaches Are Inevitable

- No organization's security is perfect – breaches are inevitable
- However, when a severe breach occurs, companies are judged by the reasonableness of their efforts to prevent and mitigate incidents
- A comprehensive, well-implemented incident response plan is critical to demonstrate that your organization takes privacy and security matters seriously

4. Privacy By Design

- March 2012: FTC releases a set of recommendations for businesses and Congress about collection and use of consumer personal information
- "Privacy by design" is central to the FTC's recommendations
  - The philosophy of embedding privacy from the outset into the design specifications of information technologies, accountable business processes, physical spaces and network infrastructures
- Avoiding "embarrassment by design"
- Tough to correct architectural deficiencies after rollout

PbD: Baking In Privacy Protections

- PbD represents a proactive, holistic approach to protecting the privacy of individuals
- Contrasts with the reactive approach associated with traditional privacy frameworks, which focus on:
  - Minimum standards for information practices
  - Remedies for privacy breaches after breaches have occurred and harm has been done
- Ontario Information and Privacy Commissioner Ann Cavoukian has been a major proponent of this concept since the 1990s

FTC's PbD Enforcement

- February 2013: FTC settles charges with mobile device manufacturer HTC America that it failed to take reasonable steps to secure the software it developed for smartphones and tablet computers
- FTC cites "permission re-delegation" issues
  - User consents to App A's use of geolocation data, but App A then shares with App B without user permission
- Settlement included comprehensive security program, conducting independent audits and reporting to the FTC for 20 years, and developing required security patches

Incorporating PbD

- Several FTC enforcement actions focus on use of default settings in collecting or sharing personal information
- Companies that design and market products capable of collecting, storing, accessing or transmitting personal information should carefully review data flows
  - Are they consistent with
    - *Product descriptions?*
    - *Legal requirements?*
    - *User expectations?*
    - *Posted privacy policies?*

5. Cybersecurity

- On Feb. 12, 2014, the Obama administration released the final version of a much-anticipated voluntary cybersecurity framework
  - Developed by the National Institute of Standards and Technology (NIST) in collaboration with stakeholders
  - At the direction of Pres. Obama's executive order one year prior
  - Focuses on protection of "critical infrastructure"

Critical Infrastructure Defined

- “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets could have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters”
- Transportation, financial services, energy and utilities, government and the public Internet qualify
- Applicability to other industries, such as healthcare, is still uncertain

Enabling and Incentivizing Adoption

- The DHS Critical Infrastructure Cyber Community Voluntary (C3) program will assist stakeholders in understanding the framework and support development of sector-specific guidance
- At present there are no incentives for compliance, but there has been discussion about tying the framework to benefits such as liability protections, grants, cyberinsurance and government contracts

The Framework

- The framework borrows from existing industry security standards and encourages organizations in the critical infrastructure sector to
  - Map out a “current profile” of cyberattack readiness
  - Pinpoint a “target profile” that reflects readiness based on an analysis of the likelihood and impact of a cybersecurity event
  - Identify “gaps” between the profiles
  - Implement an action plan to address those gaps

Beyond Critical Infrastructure

- Any company experiencing a cybersecurity event will want to be able to demonstrate that its security practices are consistent with the framework – regardless of industry sector
- Dovetails with other legal trends supporting the adoption of formal security compliance programs
- The framework should prompt increased focus on cybersecurity in US corporations at the senior executive level
- October 2011: SEC Division of Corporate Finance released cybersecurity risk and incident disclosure guidance

6. California Online Privacy

- The California Online Privacy Protection Act (CalOPPA) is a unique state law that requires
  - Operators of commercial websites and online services
  - That collect personally identifiable information of California residents
  - To post a privacy policy containing certain required elements
  - The policy must be “conspicuously” posted

Amending CalOPPA: CA AB 370

- Effective Jan. 1, 2014, CA A.B. 370 requires disclosure of a website's "do not track" (DNT) practices
- Privacy policies must now disclose whether the website or online service will honor DNT signals from Web browsers
  - Mozilla and Microsoft allow consumers to enable DNT features
- Does not require compliance with a DNT signal, just disclosure of practices

CA AB 370

- Also requires that operators include information about whether third parties may collect personal information about the California consumer's online activities over time and across websites when the consumer is using the operator's website or service
- The good news – violations of CalOPPA occur only if operator fails to correct a deficiency within 30 days of being notified of noncompliance
  - Unless failure to comply is "knowing and willful" or "negligent and material"

Amending CalOPPA: CA SB 568

- Effective January 1, 2015, CalOPPA is amended to give California minors (under 18) the right to remove information they post online
- Website operators must provide notice of the “delete” option and the fact that it does not guarantee complete removal of the content
- SB 568 also prohibits certain marketing and advertising to minors, including ads for firearms, tobacco and dietary supplements

Wagging the Dog

- National companies that collect personal information of California residents online should review their privacy policies for compliance with CalOPPA
  - Particularly in light of the new DNT requirements
  - Consider whether to comply with the new online minor statute in advance of the Jan. 1, 2015 compliance date
  - A *de facto* national standard
  - Complicates online minor privacy compliance because standard is very different from federal COPPA

7. Location-Based Services

- U.S. consumers are having a love affair with smartphones and tablets
  - One key to their popularity is their ability to run mobile apps using wireless location-based services (LBS)
  - Use of real-time and historical location data poses new privacy risks
- The sale of geo-targeted advertising alone is expected to generate more than $100 billion by 2020, according to the McKinsey Global Institute
- Privacy by design is once again critical

Questions for LBS Providers

- A business should ask:
  - What does its LBS service do?
  - What type of data does it collect?
  - Is the data shared by the LBS provider with affiliates, partners or third parties?
  - Is the data personally identifiable?
  - Will the data be shared with an online advertiser, marketer or a social media platform like Facebook? UNDERSTAND THE DATA FLOWS

Transparency About LBS

- LBS data should be treated as sensitive personal information, which means that uses of data should be transparent.
- Provide clear disclosures to consumers regarding:
  - What information is collected, retained and shared
  - The consumer's choices with regard to the data
  - If location data previously collected will be used for a new purpose, provide an updated disclosure and a new opportunity to exercise choice

User Consent

- Consumers should consent to use of LBS information
  - Use of pre-checked boxes or other default options that automatically opt-in users to location information collection are not recommended
- The location information of children under age 13 should be treated as particularly sensitive, in accordance with the Children's Online Privacy Protection Act (COPPA)
- In May 2012, the FCC's Wireless Telecommunications Bureau weighed in with a report on LBS services highlighting privacy and other issues to be considered.

8. Social Media Issues

- Social media policies are essential, both for employees using social media and for corporate social media marketing campaigns
- FTC emphasizes the need for transparency regarding social media marketing initiatives (see FTC's Endorsement Guides)
- Social media policies should clarify who owns social media accounts and contacts used by employees
- In the absence of a clear policy, a departed employee may walk away with a company's valuable social media assets

Who Owns Employee Social Media Accounts?

- Two recent cases highlight issues regarding ownership of employee social media accounts:
  - *PhoneDog v. Kravitz*, N.D. Cal., No. 3:11-cv-03474-MEJ
    - *Case settled, employee retained Twitter account but changed account name*
  - *Eagle v. Morgan*, E.D. Pa., No. 2:11-cv-04303-RB
    - *Company retained LinkedIn account, but a clear policy on ownership of social media accounts probably would have averted the lawsuit*

9. The HIPAA Final Rule and Regulation of Business Associates

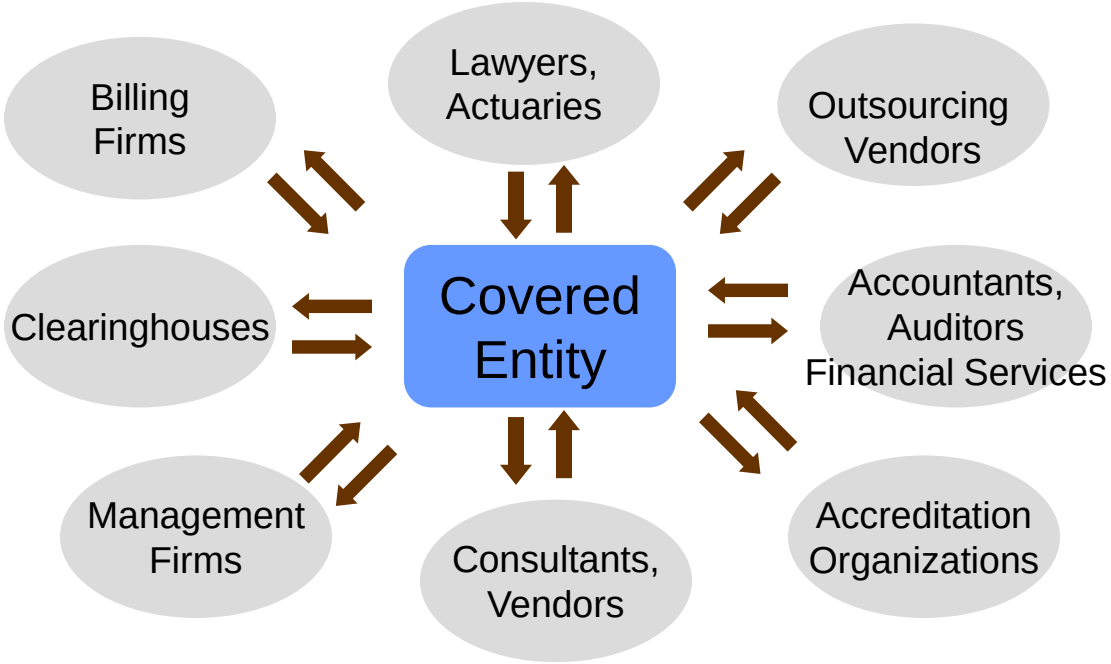
- American Recovery and Reinvestment Act of 2009 (ARRA)
  - Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH Act).
  - Marks the beginning of a new phase of health care privacy and security regulation and enforcement.
  - HHS published the HIPAA Final Rule on January 25, 2013
    - Amends the Privacy, Security, Enforcement and Breach Notification Rules
- Compliance date: September 23, 2013

HIPAA Final Rule Overview

- Extended the reach of the HIPAA Privacy and Security Rules to business associates (BAs)
- Imposed breach notification requirements on HIPAA covered entities (CEs) and BAs
- Limited certain uses and disclosures of protected health information (PHI), such as subsidized marketing communications
- Increased individuals' rights with respect to access to electronic PHI
- Increased enforcement of, and penalties for, HIPAA violations

Use and Disclosure — Who Is a Business Associate?

- A person acting on behalf of a covered entity who —
  - Creates, receives, maintains or transmits PHI
  - For a function or activity regulated by HIPAA (a covered entity function)
- BAs may also be covered entities
- This is the Final Rule's newly tweaked definition



New BA Obligations

- Prior to the HITECH Act, a BA was not directly subject to HIPAA privacy and security requirements (or HIPAA penalties).
- A BA's obligations arose solely under the terms of its BA agreement with a CE.
- BA was subject to contractual remedies only for breach of the BA agreement (BAA) (unless the BA also happened to be a CE).

BAs and the HIPAA Security Rule

- The HIPAA Final Rule requires BAs to comply with the HIPAA Security Rule's requirements and implement policies and procedures in the same manner as a CE

- Subcontractors to BAs must now also develop Security Rule compliance programs
  - Some subcontractors may face challenges in meeting this standard

BAs and the HIPAA Privacy Rule

- In contrast, the Final Rule does not impose all Privacy Rule obligations upon a BA
- BAs are subject to HIPAA penalties if they violate the required terms of their BAAs
- A BA may use or disclose PHI only in accordance with:
  - The required terms of its BAA or
  - As required by law
- A BA may not use or disclose PHI in a manner that would violate the Privacy Rule if done by the CE

Steps for BA HIPAA Compliance

1. Conducting a **formal security risk assessment**
2. Implementing **written policies and procedures** with respect to Security Rule standards
3. Providing **security training** to workforce members
4. **Amending BAAs** to include new required provisions
5. Appointing a **Security Officer** to oversee Security Rule compliance efforts
6. Adopting a **breach response plan** that tracks HIPAA Breach Notification Rule standards
7. Adopting **privacy policies** to support BA privacy obligations (not required)

10. Big Data

- What is Big Data?
  - Typically refers to the application of emerging techniques in data analytics, such as machine learning and other artificial intelligence tools, to enormous databases of personal information
  - Sources of data include smartphone GPS data, web browsing data, social networking activity, biometric data
  - Assembling powerful and surprisingly granular information about individual behavior

Too Much Information?

- Privacy laws generally regulate how a business shares information with third parties and bar uses of information inconsistent with stated business purposes
- The challenge of big data – sometimes a company may know more about a consumer than the consumer realizes or is comfortable with – even when simply servicing that consumer's account

Big Data Under Review

- January 23, 2014: White House senior counselor John Podesta officially launched a review of big data issues
  - Shortly after Pres. Obama's speech on NSA reforms
- March 2014: Podesta meets with ad industry representatives
- Some form of big data regulation seems likely, although it's difficult to say now what form it might take

Realizing the Potential of Big Data

- Companies seeking to leverage big data initiatives should
  - Be sensitive to consumer perceptions (the “ick factor”)
  - Just because it’s legal doesn’t mean you won’t be criticized
  - Ensure that you have fully secured the rights to use customer or other data for big data analytics purposes
    - *This may include getting permission to aggregate or de-identify personal information*

Questions?

Speaker Contact Information:

Reece Hirsch

rhirsch@morganlewis.com

415-442-1422