Bloomberg BNA

Privacy and Security Law Report®

What Every General Counsel Should Know About Privacy and Security: 10 Trends for 2013

BY REECE HIRSCH

A lapse in privacy can be extremely damaging to a company because it goes right to the heart of the customer relationship—privacy is personal. Raising the stakes further, privacy and security laws have proliferated in recent years at a time when (not coincidentally) more and more companies have the collection and use of personal information at the core of their business models. As a result, privacy and security law, once a somewhat arcane specialty, has become an area of law that all general counsel must be mindful of.

This article focuses on the some of the themes and trends that will most broadly impact companies in 2013. For the most part, narrow or industry-specific issues have been avoided. If this list were to be prepared next year, it would probably look quite different because if there is one thing we know about privacy law, it is that the landscape changes as fast as the versions of a popular smartphone.

1. Are You Prepared for the Broad Impact of the HIPAA Omnibus Rule? On Jan. 17, the U.S. Department of Health and Human Services released the long-awaited final omnibus rule (the HIPAA Omnibus Rule) amending the Health Insurance Portability and Accountability Act (HIPAA), introducing the most significant revisions to health care privacy law in a decade.[1] The HIPAA Omnibus Rule implemented changes mandated under the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was part of the American Recovery and Reinvestment Act.

If your company is not a HIPAA-covered entity (a health care provider, health plan, or health care clearinghouse), then why should you care about the HIPAA Omnibus Rule? Because the primary thrust of the Omnibus Rule's amendments is to extend HIPAA regulations to a host of vendors to the health care industry (''business associates'' in HIPAA parlance). If your company executes HIPAA business associate agreements with customers, then the HITECH Act will introduce significant new legal obligations and potential exposure to newly heightened HIPAA sanctions. In addition, even though there are transition provisions that may apply to existing contracts, business associate agreements entered into after Sept. 23, 2013, must include new required provisions reflecting HITECH Act obligations.

Most notably, business associates will be required to come into compliance with the HIPAA security regulations by Sept. 23, which involves conducting a formal security risk assessment, implementation of comprehensive security policies and procedures, appointment of a security officer, and conducting workforce security training. It's also important to remember that the new HITECH Act obligations will extend not only to business associates but also to subcontractors to business associates receiving protected health information of covered entities. As a result, on Sept. 23 a vast array of companies will have to become compliant with certain aspects of HIPAA—even though they may be only indirectly related to the health care industry.

2. Do Your Mobile Apps Have Appropriate Privacy Policies? California has a way of driving the national

Reece Hirsch is a partner with Morgan, Lewis & Bockius in San Francisco specializing in privacy and data security law. He can be reached at (415) 442-1422 or rhirsch@morganlewis.com.

[1] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5565 (Jan. 25, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

 ISSN 1538-3423

privacy agenda, and in 2012 the state's attorney general did it again by drawing attention to companies that have failed to post privacy policies for mobile applications. Under the California Online Privacy Protection Act (CalOPPA), Attorney General Kamala Harris issued warning letters to scores of companies believed to have inadequately addressed mobile app privacy policy issues (11 PVLR 1623, 11/5/12). Further enforcement of CalOPPA is expected, and the attorney general has made clear that California intends to strictly apply CalOPPA to mobile and social apps. On Jan. 10, the California AG also issued a controversial set of recommended privacy practices for the mobile ecosystem.[2]

The California AG's position is that CalOPPA reaches all ''operators of a commercial web site or online service'' that gather personal information about California residents. Under the act, an ''operator'' is ''any person or entity that owns a Web Site located on the Internet or an online service,'' including mobile and social apps.[3] Thus, for companies with mobile apps, the key question is not where they are located geographically but what type of personal information—if any—the app collects from its California users.

The Federal Trade Commission (FTC), in a December 2012 staff report,[4] also expressed concerns regarding child privacy and mobile apps, announcing its intention to update the Children's Online Privacy Protection Rule to address the issue. Concurrently, the FTC staff launched nonpublic investigations to determine whether entities in the mobile app marketplace are violating the Children's Online Privacy Protection Act or engaging in unfair or deceptive practices in violation of the FTC Act. The bottom line: companies with mobile apps should confirm that they have (1) crafted a compliant privacy policy with respect to personal information collected through the app and (2) posted it ''conspicuously'' in the manner required by CalOPPA—and they should do so promptly before the California AG or FTC comes calling.

3. Is Your Privacy Policy Scrupulously Accurate, Particularly With Regard to Cookies? For most companies, privacy and security practices are implemented behind the scenes, often remaining invisible to consumers—until something goes wrong. The one big exception to that rule is a company's online privacy policy. When statements made in a privacy policy are inaccurate or incomplete, the FTC may assert that such conduct is an unfair or deceptive practice violating Section 5 of the FTC Act.

Recent FTC settlements have sent a clear message that the agency will scrutinize a company's statements with respect to first- or third-person cookies, and will impose sanctions if it believes those representations are inaccurate. The FTC does not prohibit online tracking of users or the use of cookies, but information about those practices must be accurate.

The FTC has also underscored in recent settlements that companies must be cautious about all public statements that they make regarding privacy, not just those contained in an online privacy policy. Membership in self-regulatory programs relating to privacy is voluntary, but once your company represents that it is complying with an industry code, you must abide by that code or face potential liability in an FTC enforcement action. The key takeaway here is that any company with a posted privacy policy needs to review and update it regularly for accuracy to keep pace with changes in website functionality, business operations, and information collection and sharing practices.

Failure to incorporate privacy by design can lead to ''embarrassment by design.''

4. Has ''Privacy by Design'' Been Incorporated Into the Product Development Process? In March 2012, the FTC released a set of recommendations for business and Congress regarding collection and use of consumer personal information (the Privacy Framework).[5] A central tenet in the Privacy Framework is the notion of ''privacy by design,'' which is the philosophy of embedding privacy from the outset into the design specifications of information technologies, accountable business processes, physical spaces, and network infrastructures.

Recent FTC enforcement actions have made clear that privacy by design is more than a recommendation. Some companies have learned the hard way that it can be difficult to correct architectural deficiencies affecting the privacy options of consumers after rollout, and have been forced to withdraw services from the market. Failure to incorporate privacy by design can lead to ''embarrassment by design.''

Privacy by design is not a new concept. The Ontario Information and Privacy Commissioner Ann Cavoukian has been a vocal proponent of privacy by design since the 1990s. However, the principle has become a cornerstone of the FTC's enforcement philosophy. More to the point, a more proactive, holistic approach to privacy issues may pay dividends from a business perspective. Companies are recognizing that it is better to ''bake in'' privacy protections for a new product rather than attempt to patch a problem after a security breach or unhappy consumers have drawn unwelcome attention to it.

5. Have You Adopted a Formal, Written Data Security Compliance Program? Despite the uneven, patchwork U.S. approach to privacy and security regulation, a growing number of companies are now subject to some form of obligation to adopt ''reasonable'' data security measures. Among the laws mandating some form of ''reasonable security'' are (i) the HIPAA security regulations applicable to the health care industry (and which, as noted above, will extend to many vendors to the industry as of Sept. 23, 2013), (ii) the Gramm-Leach-Blilely Act (GLB Act) ''safeguards'' regulations for financial institutions, (iii) state insurance law analogs to the GLB Act Safeguards Rule applicable to in-

[2] Cal. Attorney Gen., *Privacy on the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013) (12 PVLR 80, 1/14/13), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[3] Cal. Bus. & Prof. Code § 22577(c).

[4] FTC, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012) (11 PVLR 1790, 12/17/12), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.

[5] FTC, *Protecting Consumer Privacy in an Era of Rapid Change* (Mar. 2012) (11 PVLR 590, 4/2/12), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

  PVLR ISSN 1538-3423

surance companies, and (iv) state laws governing businesses that maintain personal information of residents of Massachusetts, Nevada, and California.

Even if your organization happens to operate outside the reach of these data security laws, there is a growing consensus that implementation of a formal, written security compliance program is a best practice. In the 2012 Law and the Boardroom Study conducted by FTI Consulting Inc. and Corporate Board Member, data security was the most often cited legal issue of concern for both general counsel and directors.[6]

Since 2005, the FTC has applied the ''unfairness doctrine'' to assert that failure to employ reasonable and appropriate security measures may constitute unfair and deceptive acts and practices that harm consumers, even in the absence of specific representations by a company regarding its security practices. Although the FTC's use of the unfairness doctrine is currently being challenged in a closely watched case,[7] the FTC has in a series of recent settlements mandated comprehensive information security programs of up to 20 years accompanied by independent third-party audits. These FTC settlements are often precipitated by security breaches and, as discussed below, virtually all companies are susceptible to security breaches. Having a formal, written data security compliance program is the best way to demonstrate that your company has taken reasonable steps to avoid and promptly respond to such breaches.

6. Have You Implemented a Security Breach Response Plan? It seems that every week brings new headlines of another major security breach. In 2012, two of the largest incidents involved LinkedIn Corp. (6 million passwords breached) (11 PVLR 925, 6/11/12) and Zappos.com (24 million customer accounts compromised) (11 PVLR 158, 1/23/12). Even organizations that have made privacy and security an institutional priority are not immune from security breaches. Cybercriminals are too sophisticated, and human error and employee misconduct can never be entirely eliminated.

A significant security breach is the event most likely to bring your organization's privacy and security practices under scrutiny, whether it's from the FTC, another regulatory agency, the press, or the plaintiffs in a class action lawsuit. Therefore, companies are well served to implement a formal security breach response plan that provides a roadmap for responding quickly to a breach, mitigating potential damage, and managing any public response. You can't ensure the personal information that your company maintains will be entirely immune from unauthorized access and disclosure, but you can ensure that you have a thoughtful plan for responding to incidents when they inevitably occur.

Nearly all states have now enacted security breach laws, which are generally intended to provide for prompt notification of affected individuals so that they can take protective measures, such as ordering a credit report and monitoring accounts. A security breach response plan ensures that an organization can move quickly and efficiently in responding to a breach rather than experiencing the delays that result from learning on the fly. A security breach response plan may be distinguished from the security compliance program discussed above because it is not primarily the province of a company's information technology and security personnel. A security incident response team usually includes representatives from many key departments of an organization that must be involved in a major breach notification, such as compliance, legal, human resources, public relations, and IT.

7. The Regulatory Forecast for Cloud Computing: Partly Cloudy. Cloud computing offers enormous potential benefits for companies seeking efficient computing solutions. However, regulators are still coming to terms with the privacy and security risks associated with cloud computing. Several recent guidance documents offer a note of caution and highlight issues that companies should consider in moving forward with cloud-based solutions.

The term cloud computing encompasses a variety of business arrangements, but at its core it involves an IT provider assembling the infrastructure and resources to provide large-scale IT services to numerous customers simultaneously, including data storage and processing and delivery of software as a service (SaaS). In July 2012, six U.S. federal agencies that make up the Federal Financial Institutions Examination Counsel (FFIEC) issued a guidance document on ''Outsourced Cloud Computing.''[8] The FFIEC concluded that cloud computing should be characterized as ''another form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing.'' While some critics maintain that this is too simplistic a view, the FFIEC guidance identifies a series of due diligence questions that all companies utilizing cloud computing should consider.

The European Union Article 29 Working Group also issued important guidance on cloud computing in July 2012 in the form of opinion 05/2012, which applies to any cloud customer or provider subject to the EU Data Protection Directive.[9] Like the FFIEC guidance, the opinion advises cloud customers to maximize oversight of cloud arrangements, recommending that cloud customers conduct a comprehensive data protection risk assessment before selecting a cloud provider. The Working Group also identifies 14 specific issues that cloud customers should address in cloud service agreements. The difficulty lies in that most of those recommended terms are not contained in most current cloud service agreements, which creates an unsettled picture for cloud computing providers (most of which are based in the United States) seeking to offer services in the European Union.

8. Is the ''Bring Your Own Device'' Trend Undermining Your Privacy and Security? We all love our personal computing devices, whether they are smartphones (iPhone or Android), tablets, or laptops and, because we love them, they are increasingly finding their

[6] Corp. Bd. Member & FTI Consulting, Inc., *2012 Law and the Boardroom Study: Legal Risks on the Radar* (Aug. 2012), *available at* http://www.fticonsulting.com/global2/media/collateral/united-states/legal-risks-on-the-radar.pdf.

[7] *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365 (D. Ariz.) (11 PVLR 1069, 7/2/12; 11 PVLR 1335, 9/3/12).

[8] Fed. Fin. Insts. Examination Council, *Outsourced Cloud Computing* (July 10, 2012), *available at* http://docs.ismgcorp.com/files/external/062812_external_cloud_computing_public_statement.pdf.

[9] Article 29 Data Prot. Working Party, *Opinion 05/2012 on Cloud Computing* (July 1, 2012) (11 PVLR 1097, 7/9/12), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

way into the workplace. Although many employers have gone to significant expense to equip their workforce with devices, more and more employees are bringing their own devices to work, using them to process and store employer data in a trend known as bring your own device (BYOD). BYOD is not going away because employees don't want to carry multiple devices and they crave the most up-to-date devices available. BYOD is also attractive for employers seeking to save the expense of purchasing and updating devices and permit their employees to use the devices that they find most efficient.

Companies embracing BYOD must reconcile this trend with the countervailing pressure to implement ''reasonable security'' (see item 5 above). If a company's security policy calls for encryption of all company-owned mobile devices, but an employee uses his or her own unencrypted smartphone to store company data and that phone is hacked, then it could be argued that the company has not met the standard for reasonable security. The solution is to develop a BYOD policy that articulates effective and implementable privacy and security protections to ensure that company data maintained on employee-owned devices is not vulnerable, addressing issues such as encryption, antivirus software, and minimum system requirements and configurations.

Employers must also ensure that these BYOB policies do not violate an employee's expectation of privacy when using a device both for both work-related and personal activities. The law is far from settled in this area, but at least one U.S. Supreme Court case, *City of Ontario v. Quon*, has held that an employer's search of personal text message content on an employer-owned device was reasonable because it was conducted for a work-related purpose and was not excessively intrusive.[10] Similar issues arise when an employer requires that employees load software or configure their devices to permit remote wiping, bricking, or blocking of the device upon termination of employment. Such techniques may delete an employee's personal emails, photos, videos, and software on the device and should be implemented only if the employee has executed a clear and comprehensive consent and waiver.

9. Have You Adopted a Comprehensive Social Media Policy? The story is a familiar one. Like the cloud computing and mobile device trends discussed above, social media has, with the rise of Facebook, Twitter, and blogs in recent years, become a fact of life for many people, raising new privacy and security concerns. Companies must adopt a comprehensive social media policy in order to come to terms with the privacy risks associated with this new landscape. Employees using social media should be instructed on issues such as the protection of confidential intellectual property and trade secrets, trademarks, copyright-protected works, defamation issues, compliance with securities laws, and violating the privacy or publicity rights of individuals through the posting of photographs or video without proper releases. In addition, a social media policy should ensure that a company's HR department does not unlawfully discriminate based on information available through the social media pages of an employee or candidate.

Companies that utilize bloggers or social media in marketing campaigns should be familiar with the FTC guidance on the disclosure of paid endorsements[11] and should adopt a policy with respect to those contractors. If your company markets through social media, such as by offering gift certificates to bloggers to link to your website, you should (i) adopt a policy mandating disclosures in accordance with the FTC endorsement guides, (ii) make sure the your employees and marketing firms that you engage know those rules, and (iii) monitor what those employees and marketing firms are doing on your behalf.

The rise of Big Data raises new privacy concerns because increasingly sophisticated data analytics tools make true ''de-identification'' of personal information harder to achieve.

Another emerging social media issue involves the ownership of social media accounts that an employee uses for work purposes. When a departing employee turns over their company-issued laptop and identification badge, should the employee also turn over a Twitter, Facebook, or LinkedIn account that the employee has been using to promote the employer's business? Two current lawsuits consider that question.[12] Such controversies can be avoided through the adoption of a social media policy that makes clear that a corporate social networking account, and the valuable contacts that go along with it, is company property that must be relinquished at termination.

10. Big Data: The Next Frontier of Privacy? ''Big Data'' is the new buzzword in privacy circles and is likely to shape the privacy regulatory landscape in coming years. But what exactly is Big Data? The term typically refers to the application of emerging techniques in data analytics, such as machine learning and other artificial intelligence tools, to enormous new stores of personal information. Individually identifiable data is being assembled in ever larger and more comprehensive databases, from diverse sources such as web-browsing data trails, GPS devices, social networking activity, sensor data, and surveillance data. Big Data refers to the powerful and often surprisingly granular information that can be assembled about individuals based upon analysis of these enormous databases.

The power of Big Data was on display in the Obama reelection campaign, which was widely reported to have spent 18 months creating a new, unified database, factoring in around 80 pieces of information about each person, from age, race, and sex to voting history, and developing indexes for estimating the ''persuadability'' of particular voters. The initiative is reported to have in-

[10] *City of Ontario v. Quon*, 130 S. Ct. 2619, 2633 (2010) (9 PVLR 893, 6/21/10).

[11] Guides Concerning the Use of Endorsements and Testimonials in Advertising, 74 Fed. Reg. 53,124 (Oct. 15, 2009) (9 PVLR 14, 1/4/10), *available at* http://www.ftc.gov/os/2009/10/091005endorsementguidesfnnotice.pdf.

[12] *PhoneDog v. Kravitz*, No. C 11-03474 MEJ, 2012 BL 27330 (N.D. Cal. Jan. 30, 2012); *Eagle v. Morgan*, No. 11-4303, 2011 BL 324390 (E.D. Pa. Dec. 22, 2011) (11 PVLR 26, 1/2/12).

  PVLR ISSN 1538-3423

volved a $100 million investment in technology, and resulted in the campaign running 66,000 computer simulations per day. Obama campaign managers touted the sophistication of these tools after the election, offering a rare public glimpse into the data analytics techniques that are also being employed by many data-driven private companies.

The rise of Big Data raises new privacy concerns because increasingly sophisticated data analytics tools make true ''de-identification'' of personal information harder to achieve. Companies using Big Data should be aware of the possibility of future regulation. In December 2012, the FTC provided an indication of its interest in this area when it issued orders to nine data brokerage companies seeking information about how they collect and use consumer data (11 PVLR 1845, 12/24/12). Companies venturing into the world of Big Data should also be sensitive to the discomfort that some consumers may feel when they learn just how much a company can know about them, even when such uses of data are entirely consistent with current law.