The Year Ahead in Privacy and Data Security

2014 promises to be another eventful year in the privacy and data security fields. Although predictions are necessarily risky, there is little sign that the revelations regarding government surveillance will cease, that cyber criminals and insiders will stop hacking into personal and proprietary data and that the FTC and other regulatory authorities will stop focusing on companies' privacy and security policies and practices.

In light of the continuously uncertain waters enveloping the privacy and data security fields, how can businesses best prepare themselves for the challenges of the year ahead?

1. Government Surveillance

With further revelations from Edward Snowden likely this year, businesses that collect large amounts of data from customers and others should be prepared for continued fallout from reactions to government collection of personal data. Although the public has so far focused on the NSA, there is a direct line between business collection of data and government access and use of data. Government surveillance in many instances is only possible because the public shares large amounts of personal data with private enterprises. Given the attention that is being paid to this matter in Congress and in election campaigns,1 focus may shift from the government to private enterprises in the coming year.

2014 may also be a year when some surveillance programs are modified. Congress promises to focus on NSA practices in the coming year and the President has adopted some of the December recommendations2 of the review panel on surveillance practices. However, none of these proposed modifications would eliminate government surveillance and mollify some of the critics of the programs. Companies may suffer other repercussions from surveillance revelations. Although US Internet companies may have some success in getting the US Government to modify its surveillance practices, they are

---

unlikely to make up for ground that has been lost in the past year, particularly in the EU and in other
countries, such as Brazil,3 which have reacted strongly to US government surveillance practices. US cloud
computing companies are under intense scrutiny in the EU4 because of concerns regarding alleged NSA
access to the data pipeline and the inability of EU citizens to challenge surveillance practices. Under the
circumstances, businesses should ensure that their data collection activities, including use of cloud
providers and data transfer mechanisms, conform to best practices and applicable law. Additionally, they
should be prepared for potential fallout if they operate internationally.

2. Data Security

Given the myriad of data security threats, businesses in 2014 must continue to be vigilant in protecting
personal and proprietary information from unauthorized access from both outsiders and insiders so that
they can preserve their assets, prevent reputational harm, and protect customer relationships. If it has
not already done so, a business should have qualified personnel perform a baseline security risk
assessment regarding its operations. Such assessments address the data collected, retained, and
transferred by the entity, the sensitivity of the data, the measures protecting the data, and the applicable
legal standards. If it has previously performed such an assessment, a business should consider updating
it in light of constantly evolving threats.

Businesses should also be aware of the growing scope of security attacks5 which can come from sources
as diverse as criminal hackers, current and former employees and vendors, faulty applications, and the
increasing range of devices attached to the Internet. Businesses operating in all sectors are vulnerable to
most, if not all of these threats and should be prepared to address them proactively.

The public is increasingly aware of security incursions, as can be seen in the recent publicity given to
breaches involving retailer Target, social network Snapchat, several major health care providers, and
Adobe. Continued security incidents in 2014 may increase calls for changed security procedures for
entities accepting credit and debit cards, requirements that data be encrypted, and increased protections
of user passwords or other personal information. Businesses with customers in California should be aware
that as of January 1, 2014, user names and e-mail addresses in combination with passwords or security

---

3 Joe Nocera, *Will Brazil grant asylum to Edward Snowden?*, The Economic Times, Jan. 4, 2014,
http://economicstimes.indiatimes.com/news/international/world-news/will-brazil-grant-asylum-to-edward-
snowden/articleshow/28385822.cms
4 Stuart Lauchlan, *Europe calls for US regime change in the cloud*, Diginomica, Sept. 23, 2013,
http://diginomica.com/2013/09/23/europe-calls-regime-change-cloud/
5 Bob Violino, *The top 8 security threats of 2013*, Security Leadership, Dec. 11, 2013,
questions are considered “personal information” under California’s data breach notification law. Given past history, other states may follow California’s lead and similarly modify their data breach notification laws.

Although it is unclear whether Congress will address cyber security legislation in 2014, given current political gridlock in Washington, the Obama administration will continue its efforts to promote voluntary cyber security standards. The National Institute of Standards and Technology (NIST) of the US Department of Commerce will finalize its Cybersecurity Framework for critical infrastructure in 2014. Although it is voluntary, the NIST framework will provide guidance to businesses regarding best practices which may influence considerations as to whether an entity has “reasonable security” under existing laws. The NIST framework will also affect a wide range of businesses. In the President’s 2013 Executive Order charging NIST with developing the framework, “critical infrastructure” is broadly defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

3. Big Data
2014 is likely to see continued attention paid to both the benefits and dangers of “big data,” despite criticism that the term has been over-hyped and evidence that it is declining as a search term in Google Trends6 (which, paradoxically, is itself a big data application). Because businesses continue to collect and retain an ever greater array of data, including personal information, to promote efficiency and provide insights into their customers, the phenomenon will continue to garner news stories and attention.

Notwithstanding (or perhaps because of) these practices, there is resistance to collection and retention of personal data for some commercial purposes. One such area is the massive collection of personal data by “data brokers.” Data brokers, including companies such as Acxiom, Experian and Equifax, are entities that package and sell personal information regarding consumers for fraud prevention, credit risk assessment, marketing and other purposes. The FTC in the last few years has repeatedly signaled its interest in data brokers and their alleged lack of transparency. The FTC has announced7 that it will continue to review the practices of data brokers in 2014 and will likely release a report this year.

---

7 Prepared Statement of the Federal Trade Commission On What Information Do Data Brokers Have on Consumers, and How Do They Use It, Before the Committee On Commerce, Science, & Transportation, United States Senate, Dec.

www.mpplaw.com
In addition, the Senate Committee on Commerce, Science and Transportation, chaired by Senator Jay Rockefeller, conducted hearings and issued a staff report in 2013 that is highly critical of data brokers. Among the report’s findings were that data brokers sell products that identify financially vulnerable consumers, that they provide information about consumer offline behavior to tailor online outreach by marketers, and that data brokers “operate behind a veil of secrecy.” Claiming that data brokers’ practices are worse than those of the NSA, Senator Rockefeller has put major data brokers on notice that he is continuing his investigations in 2014.

Businesses which operate in this sector or rely upon information provided by data brokers should closely monitor developments in 2014.

4. The Internet of Things

The FTC will also continue to review the security and privacy issues associated with the Internet of Things in 2014. The FTC has called for comments by January 10, 2014 on the issues raised in its November 2013 workshop on the Internet of Things, including the privacy and security concerns associated with “smart” devices. Among the specific areas for comment are “[h]ow should the FTC encourage innovation in this area while protecting consumers’ privacy and the security of their data?” and “[a]re new use-restrictions necessary to protect consumers’ privacy?” Although the FTC has stated that its attention to the Internet of Things does not presage new regulation, it is likely to continue to use its existing powers under the FTC Act in this area. Because the Internet of Things affects a wide range of industries, including health care and medical devices, consumer products, construction and design, transportation, financial services, and environmental engineering, businesses should be attentive to potential enforcement actions and regulations in this area.

5. Health Care

It is safe to predict that privacy and data security issues in the health care sector will continue to be in the news in 2014. Indeed, on the last day of 2014, the FTC announced a proposed order with Accretive

Health, Inc., which provides services to hospitals regarding everything from registration of patients to collection of past due accounts. The FTC’s enforcement action arose when an Accretive employee lost a laptop with 20 million pieces of information about 23,000 patients, including sensitive health care information. The FTC’s investigation uncovered alleged privacy and security lapses by Accretive, including vulnerability of laptops to theft, failing to limit employees’ access to personal information, failing to secure sensitive information when there was no longer a business purpose or need, and not removing consumers’ personal information from computers after training was concluded. In reporting this settlement, the FTC recommended that businesses “adopt sensible data security policies appropriate to the kind of information provided” and not grant “all-access passes” to employees to sensitive information “without a sound business reason.”

2014 is likely to see continued attention to breaches of the HIPAA Privacy and Security rules by the US Department of Health and Human Services, as well as to issues arising from the extensions of the rules to a wide variety of “downstream” entities operating as business associates. In light of these enforcement priorities, health care providers and business associates should make certain that they have appropriate agreements in place that conform to the privacy and security rules. The FTC is also focusing on the health care sector and has announced that in a 2014 workshop, it will examine the practice of non-HIPAA covered websites, health apps and services obtaining information from consumers.

6. Mobile Applications

Mobile applications will continue to be a major focus of both federal and state regulators in 2014. One of the primary reasons for this is the growing prevalence of smartphones using such applications. In May 2013, the Pew Research Center found that for the first time, the majority (56 percent) of Americans own a smartphone, 35 percent own another type of cell phone, and 9 percent own no cell phone. The findings noted that “the cell phone is the most quickly adopted consumer technology in the history of the world.”


The FTC has announced\(^\text{14}\) that in 2014 it will examine the privacy implications of tracking consumers by businesses using signals from mobile devices. The FTC notes that such technology, which takes advantages of a device’s MAC address, creates potential privacy concerns and questions, including issues of consumer choice and transparency.

California is also likely to continue actively to enforce its laws requiring mobile applications, such as the California Online Privacy Protection Act, which requires businesses to post privacy policies, including its adherence to Do Not Track (DNT) signals. Although this enforcement effort got off to a somewhat rocky start\(^\text{15}\) with the dismissal on preemption grounds of an action against Delta Airlines, Attorney General Kamala Harris is likely to continue to focus on mobile applications.

7. Other Developments

It is risky to predict legislative enactments for the following year. With the federal government continuing to suffer from gridlock, the prospect for any new baseline privacy protection is slim, even though opinion polls indicate\(^\text{16}\) that a majority (56 percent) of Americans do not think that federal courts provide adequate protection on government data collection practices and 70 percent believe that government uses the data for purposes other than investigating terrorism.

In the absence of action from the federal government, California and other states\(^\text{17}\) are likely to continue to legislate on privacy and security. Although the bill was stopped in 2013 after an industry lobbying effort, California legislators may reintroduce a proposal for a “right to know bill” that would provide California consumers with the right to obtain copies of the personal information that a business retains about them.\(^\text{18}\) Because state laws are not consistent, businesses operating in multiple states may face issues in complying with the emerging body of state laws.

Given the greater public attention to privacy and data security, it is highly likely that the federal government will continue actively to enforce laws pertaining to privacy and security with the FTC taking...
the lead to enforce the Children’s Online Privacy Protection Act (COPPA), the Graham-Leach-Bliley Act, the Fair Credit Reporting Act, and matters relating privacy and data security under Section 5 of the Federal Trade Act. As noted, the Department of Health and Human Services will again be active in enforcing HIPAA.

About the Author
Tim Toohey is partner with Morris Polich & Purdy LLP in Los Angeles and is the head of the firm’s Cyber, Privacy and Data Security team. He is a US and EU Certified Information Privacy Professional (CIPP/US and CIPP/EU). Tim is the author of Understanding Privacy and Data Protection: What You Need to Know to be published in early 2014 by Thomson Reuters/Aspatore.