The Top 10 Privacy and Security Issues to Watch in 2014

By Kirk J. Nahra

Privacy—as a legal, political and public issue—came full circle in 2013. Once, in my law school days of yore, the privacy debate (such as it was) focused primarily on constitutional law questions involving government power versus the individual, resulting in discussion and controversy on issues such as birth control, abortion rights and disclosure of political affiliations. Then, privacy as a legal issue evolved so that the primary debate assessed the rights of corporate data holders in connection with their employees, customers and contacts. Now, with the Edward Snowden/National Security Agency disclosures, we are back to a spirited public debate about the needs of the government balanced against the rights of individuals, both at home and abroad. At the same time, this current debate has implicated the activities of corporate entities as well, as the question of what information corporate America has to provide to an ever-inquiring government takes center stage.

In addition, the Snowden affair continued a year (or is it a decade?) of data security as a legal issue, resulting from the confluence of an expanding range of security breaches and new legal and operational requirements related to technical data protection requirements. Privacy and data security are now irrevocably intertwined, with the latest addition of cybersecurity to the compliance mix.

So, we look ahead to 2014. It is clear that companies face an ever-growing range of legal requirements, business pressures and operational challenges related to privacy and data security. Chief privacy officers, who exist and participate in senior management at more and more companies, face an increasing array of concrete problems. For many, the biggest issue may not be how to comply with everything (which may not be possible, particularly in a global environment), but rather how to make reasonable sense of this mix of legal, operational and contractual challenges while at the same time effectively running an actual business. What data security and privacy issues should companies—primarily chief privacy officers, information security officials, compliance officers, general counsels, chief executive officers and boards—be paying the most attention to in 2014?

1. Snowden Fallout

The Snowden disclosures have created a series of interconnected questions on privacy and security. What actually is the government doing? How much information does the government obtain? Who is this information obtained about? What information is actually reviewed (as compared to could be reviewed)? How aggressive are the tactics to break into encrypted data? If the government can get into encrypted data, who else can? These questions will form the core of the political debate, along with numerous court challenges to the government’s monitoring practices. We can expect substantial movement (and ongoing controversy) about these issues in 2014.

For companies, we are seeing significant pushback, both in terms of a willingness to cooperate with government monitoring (as distinct from specific investigations, where typical investigative procedures likely will continue without material change) and in the aggressiveness with which companies are taking steps to protect data from government monitoring. While the focus has been on telecommunications entities and various Internet companies, we can expect the government to push for data from a broader range of entities as some of these initial sources narrow.

The biggest impact, however, in terms of compliance concerns, from these revelations will be on the reactions to the news, from foreign governments, U.S. state and federal legislators and others who are concerned

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington and a member of the advisory board for the Privacy & Security Law Report. He provides privacy, data security and cybersecurity advice to companies in a wide range of industries around the country and the world. He can be reached at 202-719-7335 or knahra@wileyrein.com. Follow him on Twitter @KirkJNahrawork.
about the steps being taken without really understanding the details. We are seeing, for example, significant negative commentary about the overall U.S.-European Union Safe Harbor Program based on these disclosures. There is a significant disconnect between the core goals of the Safe Harbor Program—which is designed to put U.S. companies on similar legal ground for protecting personal data as EU companies—and the effects of government monitoring, but that is not stopping potential changes in the international privacy regimes.

So, pay close attention to the developments with this story, and, particularly, on how those in control of legislation and regulation react to the developing disclosures, related or not, well-reasoned or not.

2. Cybersecurity

The Snowden revelations also have dovetailed with a parallel development related to cybersecurity. Beginning in 2012 and continuing into 2013, Congress and the Obama administration have attempted (with little success) to develop a legislative and regulatory approach to cybersecurity issues. While Congress developed a series of legislative proposals, none of these moved forward, leaving the administration to issue an executive order addressing the development of an overall cybersecurity framework (12 PVLR 257, 2/18/13).

The overlaps between “cybersecurity” and “data security” are important for any company to understand. Data security principles—stemming from statutes like the Health Insurance Portability and Accountability Act (for the health-care industry) and the Gramm-Leach-Bliley Act (for financial services), coupled with the FTC’s enforcement directives on data security (for everybody)—have existed for many years, and have focused on technical, administrative and physical safeguards for effective protection of personal information, whether in paper or electronic form (or any other form). These laws typically were a follow-on corollary to privacy principles dictating how these data can be used and disclosed.

Cybersecurity, by contrast, is less of a “personal information” issue and more of a “protection of our national infrastructure” issue, with undertones of national security. As noted in the executive order:

Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation’s critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.1

This means that cybersecurity concerns address how infrastructure works, how companies work together and with government, and applies to all kinds of information and operations, with no particular focus on personal data. Similarly, the critical industries involved in this executive order include not only industries that already face significant information security regulation (such as health-care and financial services), but also other industries that have little personal information and therefore are being regulated or instructed on security issues for the first time (such as manufacturing, utilities and chemicals). The ongoing developments will continue throughout 2014 (see related report).

The key issues to watch will be:

- which industries are impacted directly by the cybersecurity framework;
- how aggressive are the proposed requirements;
- will the program focus primarily on information sharing, or will it also encompass specific technical security requirements;
- how, if at all, will these requirements interact with existing data security structures; and
- how will the perceived impact on “civil liberties” impact the development of cybersecurity practices.

Companies in all industries need to focus on these developments, either as a corollary to existing regulation of security standards for the protection of personal information or as a new set of principles that affect any entity that is involved in any of the “critical infrastructure” industries, as well as useful guidance for any entity with an overall internet presence. Keep in mind that while the executive order focuses on this critical infrastructure, no company is immune from cybersecurity threats that create risks for personal and corporate information as well as ongoing business operations.

3. Security Breaches/Impact of Target

We saw in 2013 the continued evolution of an ongoing—and perhaps even expanding—problem, that of security breaches involving sensitive personal information. While various industry groups tracked hundreds of security breaches over the year, we closed 2013 with one of the largest known breaches, involving more than 40 million credit cards used at Target Corp. stores during a brief window around the Thanksgiving holiday (12 PVLR 2133, 12/23/13). Information concerning this breach continues to develop, with varying reports of exactly what information is at risk and what steps reasonably should be taken.

The magnitude of this breach is staggering—tens of millions of affected cardholders. The breach has attracted significant Congressional attention (13 PVLR 31, 1/6/14), and likely will result in investigations from multiple attorneys general at the state level as well. Yet the magnitude of this breach also distracts from the reality of most security breaches. Most are much smaller breaches, often involving dozens or hundreds of individuals, but can involve virtually any kind of business.

---

ness that maintains personal information about employees or customers. If your business has not had a breach yet, it is likely because you haven’t been looking for it.

There is no reason to think that the volume of breaches will decrease in 2014. (The magnitude of individuals affected may decrease simply because of the enormity of the Target breach.) Yet, it is clear that: (1) every business faces realistic risks of security breaches; (2) these breaches result in complicated analysis and regulatory and operational challenges, resulting from contractual entanglements and numerous state laws; and (3) many of these breaches could have been prevented through more effective security practices.

All companies should undertake a reasonable review of prominent security breaches in 2013 and in recent past years, and evaluate their own security practices with appropriate consideration of where others have faced real problems. They also should review how to minimize exposure to all kinds of sensitive data, particularly Social Security numbers.

4. The Future of the Federal Trade Commission’s Data Security Efforts

While security breaches remain a constant threat, the Federal Trade Commission, which is the “default” regulator for data security practices in the U.S., faces a direct challenge to its enforcement approach. For almost a decade, the FTC has taken enforcement action against entities that have not implemented reasonable and appropriate data security practices. Utilizing the standards established in the GLB Act, the FTC has moved ahead with dozens of cases involving inappropriate security practices, starting with the BJ’s Wholesale Club case in 2005 (4 PVLR 789, 6/20/05).

Now, the FTC faces two entities that have not accepted proposed settlements, and instead have directly challenged the FTC’s ability to engage in any enforcement activities in connection with data security. The first case, involving Wyndham Hotels and Resorts LLC, is proceeding in federal court (12 PVLR 1946, 11/18/13). The second, involving a company called LabMD Inc., is working its way through the FTC administrative enforcement structure (13 PVLR 32, 1/6/14). Both cases directly present the question of whether the FTC is authorized to engage in enforcement activity related to data security independent of specific data security statutory authority, relying instead on its general consumer protection authority. (The LabMD case also presents the separate (and important) question of whether the FTC can act in a situation where the Department of Health and Human Services has primary enforcement authority under HIPAA.)

These cases will have a substantial impact on the regulation of data security in the U.S. If the FTC wins these actions, it will continue its role as the primary regulator of data security, independent of industry segment. Its authority will reach to any company that maintains sensitive personal data about employees and/or customers (realistically meaning any company). It will be emboldened, with the ability to act without fear of later court action. And, one defense to an enforcement action will disappear, leaving the FTC to define what it views as reasonable and appropriate security practices (which, since enforcement typically happens once something has gone wrong, will truly be in the eye of the FTC beholder).

Conversely, if the FTC’s authority is struck down, one of two things (or perhaps both) will happen. First, we could see a substantial vacuum in data security enforcement authority, with increased risks to individuals. This will create a meaningful enforcement gap, both in terms of regulating U.S. data security practices and in connection with the actions of EU regulators and others to evaluate the strength of the U.S. data protection regime. The key question (and second step) will become whether this gap will finally force Congress to act, in an area where it has tried but failed to pass meaningful legislation for several years. While efforts to pass legislation continue in any event (either as a stand-alone data security bill or as part of a broader cybersecurity package), striking down the FTC’s authority will create substantial additional pressures on Congress to act. The likelihood of new legislation, perhaps much stricter legislation than the current FTC view, becomes much higher if the FTC can no longer act as a de facto data security regulator.

5. Enforcement

The court challenges to the FTC’s enforcement authority highlight an ongoing issue with privacy and security regulation: is there too much or not enough enforcement? While any company on the receiving end of enforcement certainly feels that there is more than enough enforcement, there is a widespread feeling among legislators and privacy advocates (and others) that enforcement is too limited and generally insufficient, particularly against egregious privacy or security problems.

The FTC has been the most visible regulator for about a decade. It has engaged in several dozen cases, but not more, meaning fewer than 10 in a normal year. HIPAA enforcement, while growing slightly, has been even more limited (with no enforcement at all for several initial years). GLB Act enforcement has remained at essentially zero. State attorneys general—despite having broad general authority on consumer protection, specific authority in many states under data breach notification laws and explicit new authority to enforce the HIPAA rules—have been noticeably and surprisingly absent from most enforcement possibilities.

Many people, including this author, expected broadly expanded privacy and security enforcement when the Obama administration took office. For the most part, this has not yet happened. We can expect pressure for more enforcement to continue to build, and that the combination of ongoing security breaches, increased nervousness about privacy practices and the expansion (and confusion surrounding) the “big data” concept all to push toward at least moderately more enforcement in 2014 and the years ahead.

6. EU Activities

Even before the Snowden news, the EU was embarking on a broad revision to the existing data protection environment (11 PVLR 178, 1/30/12; 12 PVLR 2105, 12/16/13). The EU Data Protection Directive (95/46/EC) has been the primary provision guiding the development of privacy law worldwide. It has become the starting point in the debate for the laws of many countries outside the EU. It has forced the development of the
Safe Harbor Program, and the ongoing challenges of transferring data to and from Europe and around the world.

The proposed revisions already were going to tighten the existing model. Penalties for violations could grow enormously. Privacy protections would be expanded. And, in general, the compliance regime for the use and disclosure of any personal data involving EU residents would become much more complicated.

While the EU process is a long one, the Snowden revelations have imposed a new concern in the eyes of the EU regulators and policy makers. There now is significant pressure to abandon or revise the Safe Harbor Program and to otherwise tighten up disclosures of data to the U.S. and outside of the EU, for fear that the U.S. government will access this data (even though the Safe Harbor is directed at the participating companies entirely) (12 PVLR 2104, 12/16/13). While the ultimate fate of these developments is still unclear, we know for sure that the EU data protection regime will become considerably tougher, and that this change will impose significant operational and contractual confusion for companies around the world.

7. Do Not Track

For several years, the do not track concept has been at the forefront of an effort to revise U.S. privacy law on the Internet. The do not track idea combines a general nervousness about marketing and behavioral monitoring with overall concerns about the “unknown” on the Internet and the rise of “big data.”

So far, however, do not track has been an idea without a clear design or goal and with dramatic tensions between technological opportunity and obligations, along with the need to balance reasonable activity on the Internet with responsible privacy protections. The process clearly has stalled, and now may be overtaken by technological developments. California, a state often unwilling to wait for technology to develop, has implemented a new law requiring certain privacy statements about do not track compliance (12 PVLR 1720, 10/7/13), although it is clear (at a minimum) that there may be no complete way to meet all of the requirements of this law or appropriately define everything the law could apply to.

So, we will see, in 2014, continued exploration of the do not track concept, as a topic of debate and a possible path towards new privacy regulation. This development perhaps will be less important for what actually results—which likely will be nothing beyond new technology—and the proxy role that do not track is playing in a broader reevaluation of Internet privacy and broader concerns about how personal behavior can be used to profile and evaluate individual activity.

8. BYOD and Mobile Devices

The other key technology development to watch in 2014 is the ongoing evaluation of how to regulate mobile devices and the related concerns about how companies can effectively manage how their data are used on mobile devices. From a regulation perspective, the effort to regulate mobile devices is caught up in the same problem facing many new technologies: extensive and swift development of technology, with capabilities well beyond what went before, and a late blooming and continually lagging effort to develop appropriate regulation without stifling economic and technological opportunity. These concerns in the U.S. are magnified by the regulatory vacuum (which the FTC is trying to fill, along with others) and the nonstop growth in capabilities of mobile devices.

From a corporate perspective, the question of what new regulations are coming for mobile devices is probably less important than the current issue of how to manage the use of these devices. Companies that have not yet developed an appropriate policy for the use of mobile devices have in fact adopted a policy—they are letting data be used and disclosed in largely unpolicied ways. Every company needs to review their overall strategy for mobile devices, whether through a formal bring your own device (BYOD) program that provides and supports particular technology, and/or a broader program that addresses how employees and others use mobile devices, with or without the company’s formal support. These devices create a broad range of concerns, ranging from theft of personal and corporate data, overall employee monitoring strategies, new and expanding risks from security breaches, the need to investigate and mitigate security breaches and a wide variety of lesser concerns about how employees use devices to perform their jobs and use and disclose data. While there are few “right” answers, companies must evaluate this issue and develop an approach that appropriately balances the enormous risks with an environment that (1) recognizes the reality that these devices will be used by a growing number of employees and (2) the benefits of a mobile work force.

9. Insider Access

As discussed above, security breaches remain an ongoing concern, related both to changes in technology and more “low-tech” situations involving paper records and lost or stolen equipment. We also are seeing, in all sorts of industries, one specific security concern that companies need to address: breaches resulting from improper behavior by employees who need access to data to do their job but then misuse this data for an inappropriate purpose. The health-care industry has seen the biggest set of these breaches, but they can apply to any industry where there are lower-level employees (customer services, intake, data entry, etc.) who need access for their jobs, often wide-ranging access, but in some instances will misuse data to commit identity theft, engage in fraud or otherwise misuse or wrongfully disclose sensitive personal information. As with any kind of security control, companies are faced with the need to take steps up front to reduce risks, and then engage in ongoing activities to monitor and investigate.

In this situation, it is often difficult to properly control front-end access to data. Customer service representatives, for example, need access to information about every customer, because you never know who will call. Companies should always look to streamline this access in any way reasonably possible, especially to sensitive data. However, where this is not a complete solution (which will typically be the case), it is crucial to have the tools for both ongoing monitoring and effective investigation in the event of a specific problem. This is a problem that is facing companies in virtually every industry and that is creating actual ongoing risks...
to personal information, with a large enough number of specific identifiable situations to require aggressive action. 2014 will be a year of improving data control efforts and improving the ability of companies, in real time, to stay on top of employee behavior and act quickly in the event of identifiable concerns.

10. Global Confusion and Complexity

The last key issue to watch in 2014 is a result of this overall set of concerns—the increasingly complicated morass of data protection obligations across the globe. We will continue to see the emergence of new national laws in countries that have not had them, and revised or broadened versions in many countries that already have existing laws. This increasing volume and detail of laws is being combined with technological developments (including but not limited to cloud computing) where national boundaries increasingly make little sense in connection with data protection. Enforcement agencies in countries around the world will have the ability to investigate where they want. Global businesses will increasingly seek to impose more complicated contractual requirements on business partners and others, resulting in an overall more complicated data transfer process, creating confusion rather than simply protecting data better.

While it is possible, at some point in the future, that this web of conflicting and overlapping rules will result in a more consistent set of overriding principles, we are not seeing this movement yet. Instead, we are seeing more laws and rules, coming from more places, covering a wider range of activities and data and imposing an increasingly broad set of compliance obligations. 2014 will be a good year to be a knowledgeable, practical privacy officer.

Conclusions

Continuing a trend from the past decade, more businesses in more industries and in more countries need to pay careful attention to privacy and data security issues. Compliance needs to be a prominent concern, whether driven by enforcement risk or the desire to meet global standards. Increasingly, however, the challenge for data privacy officers and others involved in privacy and security compliance will be the need to make practical sense of this jumble of regulation to allow an appropriate balancing test that meets specific regulatory and legal obligations in a way that permits businesses to still operate effectively. Understanding how to protect a company and its customers effectively, whether by meeting all potential standards or simply by being smarter about data protection practices, will require substantial thought and experience on data privacy and security issues. These questions are becoming more complicated with time, not less, and will continue to play a more prominent role in business activity as regulation multiplies and the opportunities for reasonable use of data continue to grow.