wiley

NEWSLETTER

What You Should Be Watching for in 2014

January 2014

Lots of privacy and data security news kept us busy in 2013, and there's no slowdown in sight. What should chief privacy officers, information security officials, compliance officers, general counsels, CEOs, and Boards of Directors be looking for in 2014? (Note—for an expanded look at the privacy and security issues raised in this article, see Nahra, "The Top Ten Privacy and Security Issues to Watch in 2014," *Bloomberg BNA Privacy and Security Law Report* (Jan. 13, 2014)).

Snowden Fallout

The Edward 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?

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 about the steps being taken without really understanding the details. We are seeing, for example, significant negative commentary about the overall U.S. Safe Harbor program based on these disclosures. Pay close attention to the developments with this story, and on how those in control of legislation and regulation react to the developing disclosures, related or not, well-reasoned or not.

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 (EO) addressing the development of an overall cybersecurity framework.

The key issues to watch will be:

- Which industries are impacted directly;

- 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" affect the development of cybersecurity practices.

Companies in all industries need to focus on the development of the EO framework, whether 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—while the EO focuses on this critical infrastructure, no company is immune from cybersecurity threats that create risks for both personal and corporate information as well as ongoing business operations.

Security Breaches/Impact of Target

We also saw in 2013 the continued evolution of an ongoing—and perhaps even expanding—problem: security breaches involving sensitive personal information. We closed 2013 with one of the largest known breaches, involving more than 40 million credit cards used at Target stores during a brief window around Thanksgiving. The magnitude of this breach is staggering—tens of millions of affected cardholders. The breach has attracted significant congressional attention, and likely will result in investigations from multiple Attorney Generals at the state level. But this was one of many breaches in 2013, affecting all industries and a wide variety of security risks.

All companies should undertake a reasonable review of prominent security breaches (both large and small) in 2013 and in recent past years, and evaluate their own security practices with appropriate consideration of where others have faced real problems.

The Future of the Federal Trade Commission's Data Security Efforts

The Federal Trade Commission (FTC)—the United States' "default" regulator for data security practices—faces a direct threat 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. Now, the FTC faces two entities that have not accepted a proposed settlement, and instead have directly challenged the FTC's authority to engage in any enforcement activities in connection with data security. 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, across most industries, and likely will be emboldened with the ability to act without fear of later court action. 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 would create a meaningful enforcement gap, both in terms of regulating U.S. data security practices and in connection with the actions of European Union (EU) regulators and others to evaluate the strength of the U.S.

data protection regime. The key question 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. 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.

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 with respect to egregious privacy or security problems.

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.

EU activities

Even before the Snowden news, the EU was embarking on a broad revision to the existing data protection environment 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.

The Snowden revelations have imposed a new concern in the eyes of the EU regulators and policymakers. 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. While the ultimate fate of these developments is still unclear, we know for sure that the data protection regime will become tougher, and that this change will impose significant compliance obligations and create substantial operational and contractual confusion for companies around the world.

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. So far, however, it's been an idea without a clear design and 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.

We will see in 2014 continued exploration of the Do Not Track concept. Companies will need to comply with a new California law addressing Do Not Track technology that took effect on January 1, 2014. Also, look for a broader impact on technology and best practices due to the proxy role that Do Not Track is playing in a

broader re-evaluation of Internet privacy and broader concerns about how personal behavior can be used to profile and evaluate individual activity.

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 is used on mobile devices. 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 behind effort to develop appropriate regulation without stifling economic and technological opportunity.

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. Every company needs to review its 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. 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 with (2) the benefits of a mobile work force.

Insider Access

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. 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. 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.

Global Confusion

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. 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. 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 morass 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, 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.