THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor: Kirk J. Nahra, CIPP/US
January-February 2012 • Volume 12 • Number 1

## The 2012 privacy forecast

### What to watch for in privacy and security in 2012: The top five

By Kirk J. Nahra, CIPP/US

Privacy and security remain in the news almost constantly. From cybersecurity issues involving global superpowers and security breaches affecting patients, consumers or employees to the debate about what privacy rights individuals have against businesses and the government, numerous issues involved in the policy debate currently affect businesses and individuals on a national and global basis. What are the top five key areas to watch in this debate in 2012?

1. **Will Congress finally act on privacy or security?**

Congress has been debating a broad privacy law since the dawning of the Internet era in the mid-1990s, with virtually no consensus. Congressional interest has waxed and waned, depending on competing pressures; particular instances of perceived privacy or security violations, and a wide variety of other factors. For the first time since this debate began, it now appears that Congress is more likely than not to pass broad privacy and security legislation. As a prediction, this "more likely" proposition means somewhat more than 50 percent, meaning there are still significant questions as to whether there will be any final legislation. Moreover, the substance of any enacted legislation is very much up in the air. If this increased probability actually results in new legislation, however, this legislation will be a game-changer for the privacy and security community. If legislation is passed, it will have broad applicability essentially across all segments of American business and will require virtually all companies to pay close attention to protecting the privacy and security of personal data.

There are three "big picture" topics being debated for this legislation. First, most of the competing bills address overall information security practices. If legislation is enacted, it will include a mandate for all businesses that collect or maintain personal information about customers, employees or others, regardless of industry sector, to implement reasonable and appropriate protections for this information. While the precise details of this security framework are still being debated, it is hard to see how broad legislation could be passed that would not incorporate significant new security requirements.

Second, most of the bills also include nationwide security breach notification provisions. While 46 states currently have breach notification provisions protecting their residents, and certain industries already face federal breach notification standards—most noticeably the healthcare industry, the proposed legislation will provide a nationwide standard for notification in the event of security breaches involving sensitive personal information.

The key variables in this debate involve the scope of the protected information; the applicability of a "risk-of-harm" threshold before notification is required; the steps that must be undertaken in connection with a risk-of-harm assessment; and most importantly, whether this federal standard will preempt the confusing and often inconsistent matrix of state laws. Again, if legislation is passed, it likely will include a provision dealing with security breach notification.

Third, there is the ongoing possibility of "privacy" legislation, although there is far less agreement on the need for any such legislation and the scope of the appropriate protections. Privacy provisions could cover "narrower" topics—such as changing the Children's Online Privacy Protection Act provisions protecting children—or broader provisions addressing EU-style universal protections or creating new rules for overall Internet privacy protection. There is no legislative consensus on privacy issues at this point.

Accordingly, there is a better-than-50-percent chance that we will see significant new federal legislation in 2012 addressing overall security standards and security breach notification, with a far lower chance that the legislation also will address broader privacy topics. In any event, if legislation passes, it will be the first time that there has been broad legislation in this area applicable to wide ranges of personal information in all contexts and all industry segments. This legislation would impose formal legal requirements on virtually all companies—I typically describe the covered companies as any that have either employees or customers—going beyond the "best practices" that have developed over the past decade.

**2. Will the litigation floodgates be opened?**

Over the past decade, as privacy issues have taken on increased visibility in the public debate and security breaches have made news across the country on a regular basis, we have seen a wide range of class-action cases filed involving privacy and security issues on behalf of various groups of individuals. In recent years, these cases have been dominated by class allegations involving security breaches. For the most part, the courts have drawn a long and growing line in the sand, rejecting class-action cases in connection with security breaches absent a clear allegation of specific and identifiable actual damage to the potential class members. These decisions have been clear and consistent, in state and federal courts across the country.

Yet, the plaintiffs' class-action bar clearly has not given up on security breach cases. In fact, we are seeing cases being filed with increased frequency, particularly where a breach involves lots of people and has been well publicized. Often there have been multiple suits, with some breaches resulting in more than a dozen separate lawsuits, typically filed within a very short time following the announcement of a breach.

To date, class-action defendants in security breach cases have faced adverse publicity, and clearly have incurred defense costs, but have typically been able to secure claims dismissal at relatively early stages of the proceedings. Some cases have taken longer, particularly where appeals of dismissals have been involved, but there have been no real blockbuster cases where courts have found that clear, demonstrable damages have been alleged or proven on a class-wide basis. This question of actual damages has been the key limiting factor in the overall area of class-action litigation over privacy and security breaches.

It will be well worth watching two key cases in 2012 to see if this landscape changes. The first, involving the Hannaford Brothers grocery store chain, creates a slight crack in the wall of cases dismissed for lack of actual damage. In the First Circuit's recent decision, *Anderson v. Hannaford Brothers Co., 659 F.3d 151, 2011 WL 5007175 (1st Cir. 2011)*, the court affirmed the dismissal of several claims against the chain arising from a security breach involving hacker access to credit card numbers. However, it reversed the dismissal of two counts, based on negligence and breach of implied contract, allowing these claims to proceed. Primarily, this was based on specific

facts from this incident not typically present. Sophisticated hackers broke into the system to take this information and actually used it in some situations. This gave more credence to the possibility of damage and affected the court's views about the appropriateness of recovering the costs of mitigation steps. While not definitive on the ultimate issues, and presumably dependent at least in part on these particular facts—which wouldn't be present, for example, when a computer is lost or stolen at random, this decision leaves open the possibility that the district court will find that actual harm has been asserted—even if only applied to mitigation costs—or that the case will proceed far into discovery and perhaps trial before this question of harm can be resolved. If Hannaford moves in this direction and is followed by other courts, there could be a sea change in class-action litigation involving privacy and security claims.

The second case to watch goes in a different direction but addresses the same issue of actual harm. In this case, recently brought against Sutter Health in California, the class is relying on a California law that provides statutory damages as a means of avoiding the need to show any actual harm. The Sutter case involves the theft of a desktop computer from a Sutter office, despite the repeated assertions in the complaint that the theft involved a laptop. There has been no report to date of any misuse of any information from this computer. Nonetheless, the class-action complaint asserts statutory damages under California law, seeking $1,000 for each of the more than four million potential class members. Thus, this complaint seeks $4 billion in statutory damages, without any showing of any harm whatsoever. This threat of statutory damages is somewhat similar to the spate of lawsuits brought under the Fair and Accurate Credit Transactions Act statute seeking statutory damages for disclosure of certain information on credit card receipts, again without any assertion at all of actual harm. Those cases became so numerous and so burdensome—and the potential damages so high—that Congress stepped in with legislation that removed most of these cases from the court dockets.

It will be critical to watch whether the Sutter claim, or a similar case filed recently against UCLA Medical Center, creates another environment—so far limited to California—where the damages hurdle can be sidestepped through allegations of statutory damages. These statutory damage claims could then lead to a wide range of lawsuits where harm may not be a relevant factor in the litigation.

Taken together, Hannaford and Sutter guarantee an interesting year on the litigation front. If these cases produce a new landscape for security breach cases, then the costs related to security breaches—and the risks for any company—will multiply. This would affect not only litigation costs but also the related complexity of negotiations with vendors and others over these costs, creating significant burdens on virtually all companies without necessarily creating any benefit, other than potential windfalls for class-action plaintiffs.

3. **Will the international environment change, and how?**

The debate in Congress, at one level, is about whether the United States will move any closer to the privacy model established by the European Union (EU), which has set the primary trend for the rest of the globe. Prompted by the EU's privacy approach, countries around the world have embarked on their own privacy regulatory schemes, creating widespread confusion and complexity for any business operating on an international scale. Over time, many companies have learned, to some degree, to manage these complexities and have begun to settle into an uneasy comfort with the confusing, overlapping and sometimes inconsistent global privacy regulations. At the same time, the EU model has continued to create its own concerns, as the U.S. Safe Harbor program only solves certain cross-border issues and does little to address true global exchanges of personal information.

Now, the EU seems primed to revamp its overall approach. We are seeing the first tentative indications of what a new world order might look like if the EU changes its approach. The EU approach is both positive and negative for industry. First, there is an effort to streamline some of the means of achieving compliance through improved

processes related to binding corporate rules and the use of model contract clauses. Presumably, these changes will supplement the Safe Harbor program rather than supplant it, but that is not entirely clear at this time.

In addition, however, the EU seems to be moving aggressively toward new standards in certain areas, including increased consent for internal usage, tougher security standards and various other new provisions that will increase the obligations imposed on companies operating in the EU and, to some extent, elsewhere. These changes will advance in 2012, although it is not expected that the developments will be final until future years.

At the same time, the EU's steps, even in draft form, will affect both ongoing business transactions and operations, along with actions by non-EU countries. While global commerce continues to increase, and certain developments—including the Internet generally and the development of cloud computing specifically—may make certain international borders largely irrelevant for data flow, there seems to be little inclination in governments around the globe to simplify, streamline or standardize privacy and security compliance, with resulting complexity, challenges and legal risk for all companies with any international presence.

**4. What's happening with healthcare, and why does it affect everyone?**

While most of these top developments affect the full range of corporate America, our next issue to watch is focused on the healthcare industry. The Health Insurance Portability and Accountability Act (HIPAA) privacy and security structure has created the most detailed and complex set of privacy and security requirements at the federal level since the privacy rule first required compliance in 2003. Now, following passage of the Health Information Technology for Economic and Clinical Health (HITECH) law in 2009, we—finally—will see in 2012 the issuance of final HITECH regulations that will kick off the full Version 2.0 of the HIPAA era.

But this development is critical because HIPAA/HITECH no longer is limited in any meaningful way to the healthcare industry. Instead, two key developments—one not yet set in stone—demonstrate that these changes will affect an enormous range of companies across the country, many of which have no obvious tie to the healthcare industry. First, one of the key changes from the HITECH law concerns the applicability of the privacy and security rules to "business associates," which are service providers to the healthcare industry. These entities have had contractual obligations for many years, but the new law requires that these business associates face legal obligations directly under the rules as well. So, through this step, which is being implemented in rules that are not yet final, the scope of HIPAA now will extend to any company that provides services to healthcare companies that involve any healthcare information—as well as creating complex negotiations and various other debates about whether healthcare information really is involved in providing the service.

The second step expands this circle even more. In the proposed regulations applying this statutory language, the Department of Health and Human Services (HHS) proposed to expand coverage not only to the companies that contract directly with the healthcare companies, which clearly are encompassed by the statutory changes and would know that they are contracting with healthcare companies, but also to any downstream vendor that contracts with those service providers, and on down the chain, indefinitely. This creates a potentially never-ending chain of contractual entanglements that impose legal obligations—even in situations where the downstream vendors may not have any idea they are involved in information from a healthcare company. This requirement would apply not only to specific "subcontractors" that perform a part of the work assigned to the business associate but also to a wide range of general service providers to the business associate; e.g., accounting firms, law firms, consultants, auditors, that perform work generally for the business associate that is not necessarily tied to any particular client or project. And, because the primary legal obligation imposed by these new provisions is to follow the full scope of the detailed and complicated HIPAA Security Rule, companies will be faced with a choice even before they receive any healthcare information about whether to take on the task of

revamping overall security programs. So, we'll be watching closely how these final rules play out and also how far down the corporate chain these rules apply. It is quite likely that the HIPAA rules will become almost a de facto national security standard, if the reach of these rules applies to anyone in the contracting chain.

5. **Will we finally see more enforcement?**

With all of this activity in the legislative, regulatory and courtroom arenas, the last key domino to watch in 2012 is whether we see a new era of privacy and security enforcement. Currently, many agencies at the federal level, including the Department of Health and Human Services, the Federal Trade Commission (FTC), the Department of Justice, the Federal Communications Commission and all of the federal banking regulatory agencies, have significant privacy and security enforcement authority. Each state's attorney general (AG) also has specific authority under either particular laws—such as HIPAA—or general state consumer protection authority. And while there have been a number of high-profile enforcement cases in recent years, the overall breadth of enforcement has been modest. The banking agencies have done almost no enforcement. HHS has done little HIPAA enforcement—and has faced significant congressional criticism for its lack of enforcement activity. The FTC has engaged in some high-profile actions, including recent cases against Google and Facebook, but the volume of FTC cases has been modest and the available sanctions are very limited. State AGs also have been surprisingly quiet, other than in a handful of cases mainly involving security breaches.

So, the issue to watch in 2012 is whether this perfect storm of new actions—ranging from new legislative provisions to higher penalty options under HIPAA to increased reporting of security breaches to congressional and public pressure—will result in new and more extensive enforcement in 2012. Privacy advocates have argued that it is only through more aggressive enforcement that companies will finally pay sufficient attention to privacy and security issues. While companies across the country clearly have expended substantial time, energy and money in support of privacy and security initiatives, it also is clear that enforcement has been more limited than most expected. So, we'll be watching whether this Administration—and the various other enforcement agencies—takes more aggressive action on privacy and security compliance in 2012.

**Conclusion**

Privacy has been an important issue for companies in many industries for many years. At the same time, for companies outside of specifically regulated industries such as health care and financial services, privacy compliance has been a business choice, driven by marketing imperatives or particular incidents. For many companies, privacy has been an issue to ignore except where absolutely necessary.

We can expect this to change in 2012. Whether through current provisions addressing security breach notification, which are not industry-specific, or through enhanced legislation and enforcement activity, privacy and security should be a high-level concern for any company—assuming it collects, uses, stores, discloses or maintains personal information about its employees, customers or others. If a company doesn't have customers or employees, these rules will have less impact on it. But, for the rest of the companies across the country, in every industry, we can expect 2012 to be the year that privacy and security move from being "good things to do" to specific legal obligations with important consequences for a failure to meet defined responsibilities.

***Kirk J. Nahra,*** **CIPP/US,** *is a partner at Wiley Rein LLP in Washington, DC.* *This article was published in the November 2011 issue of* Privacy In Focus *and is reprinted here with permission.*

**_The Privacy Advisor_ asked, what data privacy issues will you be watching most closely in 2012?**

"**Key issues** to keep me busy in 2012 include the revised EU legislative framework (upcoming draft regulation), implementation of the revised e-privacy directive by the Member States (including the controversial cookie rule), the transatlantic dialogue as well as the U.S. federal legislation under preparation and, more globally, the expansion of privacy rules across the world and the increasing need for standardization for the development of seamless cloud and other services."
—***Tanguy Van Overstraeten**, Partner, Linklaters LLP, Brussels*

"**2012** will be rich in privacy issues of top line interest. In no particular order, I will be watching:

• The public debate over Do Not Target (most so-called do-not-track proposals are a misnomer because they propose some controls over targeting while still tracking)
• Emerging issues in mobile and geolocation
• Governance of cloud computing (how to ensure the consumer is just as well protected in a multi jurisdictional, long supply chain environment)

- eHealth in Australia (in particular, the Personally Controlled eHealth Record and the surrounding governance
- Privacy law reform in Australia (will any legislation be introduced in 2012)?
- Privacy law reform in the rest of the world (Europe, U.S.A,Malaysia, Philippines, Singapore, Japan, elsewhere)"

—***Malcolm Crompton, CIPP/US**, Managing Director, Information Integrity Solutions Pty Ltd, Sydney*

"**2012** is the year to up-end well-settled privacy law. The primary EU data protection directive will be replaced with
significant changes; OCR will issue omnibus HITECH regulations; the CFPB may begin work in earnest having gained a director, and omnibus federal legislation may preempt much of the state privacy law that has driven compliance efforts in the U.S. But never fear, the old drivers (security breaches, mobile devices and social media) are still going strong…"
—***Elizabeth Johnson**, Partner, Poyner Spruill, LLP, Raleigh*

"**I'll be** keeping close tabs on the implementation of the new Canadian anti-spam law and when it finally takes effect. It impacts us, as we send out e-mails to our members and customers from time to time and, accordingly, we've spent a lot of time preparing for it."
—***Nicholas F. Cheung, CIPP/C**, Director, Program and Publication Development, The Canadian Institute of Chartered Accountants, Toronto*

"**The business** associates/partners of organizations will receive unprecedented increased scrutiny and penalties as the breaches they cause continue to increase dramatically. As a result, these businesses will start implementing more privacy protections, and will be monitored by their business clients, more than ever before. In addition, the at least five proposed rules for HIPAA/HITECH will be finalized in 2012…finally! And, utilities will more proactively and publicly address the privacy concerns of smart meters, and more directly point to the need for third parties that consumers directly share HAN data with (typically not subject to current or proposed smart grid privacy rules) to do more to preserve privacy in the smart grid."

—***Rebecca Herold, CIPP/US****, The Privacy Professor, Rebecca Herold & Associates, LLC*

"**There are** many issues on which we will have to focus in 2012, especially now that the Secondary Regulations to the Federal Law on the Protection of Personal Data held by Private Parties have been published. These issues include disseminating—primarily among data controllers—the importance of embedding the principles of privacy and data protection into their day to day activities; analyzing data processing mechanisms in order to determine the need of implementing a privacy notice or a compensatory measure (considering the number of data subjects and the aging of the data); establish the responsibilities and obligations of the different persons working in or together with a data privacy department; develop access, rectification, cancellation and objection formats and other mechanisms that will facilitate the exercise of these rights; counsel in connection with the management and response to access, rectification, cancellation and objection rights applications and determine the extent of such rights (for example, does the right of access mean that you have to provide a copy of the document where the data is included, etc.); work on the identification and implementation of security measures that will prevent damage to personal data, etc."
—**Rosa María Franco**, Partner, Basham, Ringe y Correa, Mexico