Bloomberg BNA

Privacy and Security Law Report®

The Top Ten Privacy and Data Security Issues to Watch in 2013

BY KIRK J. NAHRA

Top ten lists are both fun and really hard to do. David Letterman has made a living with them for more than 20 years. Some lists—the best books of the year, for example—are purely personal, and have the benefit of being selected from a new crop each year. Last year's books need not apply.

For privacy and security, the challenge is different. Some issues are very important and simply do not go away. The ''imminent'' Health Insurance Portability and Accountability Act (HIPAA) rules will be on this list for the third straight year (and we haven't even seen them yet). Other issues rise or fall depending on politics, international relations and new technological developments. The popular media makes certain issues jump in visibility, almost randomly, if there's a catchy hook. Moreover, while all companies are touched by some set of privacy and data security issues, the latest developments on certain laws (for example, new privacy notices under the Gramm-Leach-Bliley Act) are important to some but entirely irrelevant to many others.

So, this list of the top ten privacy and security issues to watch in 2013 is driven by my own scientifically and meticulously selected review of the issues that will matter the most to the most people in 2013, based on a proprietary model peer-reviewed by a respected panel of experts (or, at least, the things I think will be important in 2013). Here goes.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, where he specializes in privacy and data security issues. He can be reached at (202) 719–7335 or knahra@wileyrein.com.

1. The Eagerly Awaited HIPAA/HITECH Act Rules

Let's get this one out of the way. For the third year in a row, the Department of Health and Human Services (HHS) definitely—guaranteed—without fail (or at least pretty likely) will issue the long overdue regulations implementing the Health Information Technology for Economic and Clinical Health Act (HITECH Act). For those of you who may have forgotten, the HITECH Act—passed in February of 2009—made specific changes to the text of the HIPAA Privacy and Security Rules. The text of this legislation specified that these changes would be effective one year after passage of the law (meaning February 2010). However—for reasons that have never been clearly explained—the Department of Health and Human Services made clear—in July 2010, several months after these provisions were to be effective—that in fact the statute meant nothing, and that no changes would take effect until a new regulation was issued. We've been waiting since then. The July 2010 announcement came in the course of the proposed regulation addressing these changes (9 PVLR 1007, 7/12/10). Since then, nothing, other than various now inaccurate predictions and a lot of waiting and confusion. The only part of the HITECH Act that is in effect—through an ''interim final regulation'' (8 PVLR 1227, 8/24/09)—is the breach notification provision, which already has had an enormous impact on the health care industry.

Waiting aside, these new rules may end up being somewhat anticlimactic. The proposed rule actually said very little, other than transferring the HITECH Act statutory language into the regulations. We knew from the statute almost all of what the proposed regulation said (even though it took a year and a half to get out). There was little interpretation and little change beyond what the HITECH Act mandated. HHS made some very minor changes based on its almost ten years of overseeing the HIPAA regime, but these changes appear to have virtually no importance (unless you have been dead for more than 50 years and your privacy rights have now been decreased).

In addition, the statute itself addressed or modified very few HIPAA provisions. The major impact of the rule will be on HIPAA business associates—contractors

 ISSN 1538-3423

and service providers to the health care industry—who will need to follow new requirements including (most onerously) the HIPAA Security Rule. This impact will flow downstream as well, to all subcontractors and others who access any HIPAA-protected information. But the most important impact of these changes—once they are finally issued—will be to finally stop the confusion, anxiety and uncertainty that have plagued the health care industry during this delay. If nothing else, the issuance of these new rules will be an important reminder to the health care industry that it needs to constantly pay close attention to the privacy and security of health care data.

Key Takeaways

- Business associates should start compliance efforts now, particularly for the HIPAA Security Rule.
- Everyone in the health care industry needs to pay close attention to potential breaches.
- Watch for any wild cards in the final rules—topics that haven't been addressed in the statute and the proposed regulation.

2. Legislative Changes

The possibility of new privacy and security legislation continues to fascinate legislators at the state and federal level. For the past several years, the legislative debate on privacy and security brings to mind Shakespeare as much ado about nothing. Nonetheless, we are likely to see considerable energy spent on development of potential privacy and security legislation. And while the odds of any significant privacy legislation getting through Congress are quite low, the mere discussion of many of the issues begins to affect behavior on a broader level. In addition, developments at the state level are much more subject to current events or legislative whim, such that the likelihood of new privacy legislation at the state level is always significant.

The most significant legislative topics in recent years have fallen into three significant categories: *privacy* (meaning specific restrictions on how personal information in a variety of contexts can be used), *security* (typically dictating specific technical safeguards for personal information) and *breach-related issues* (focused primarily on adding new—and often confusing, inconsistent or unnecessary—details to the various state breach notification laws). Congress has waded into these territories, through a variety of proposals in each category. Most of the legislation has been introduced to make a particular political point or address a specific topic of concern. There has been little traction for any new significant privacy legislation in Congress (although there is a somewhat increased likelihood of legislation addressing issues such as geolocation). The concepts of national data security legislation and national breach notification legislation have moved somewhat further along the legislative spectrum (and may be linked to the passage of legislation on cybersecurity issues), but we have seen little significant movement from Congress on these issues in recent years. Given the current overall state of debate in Washington, it would be surprising to see meaningful privacy or security legislation emerge in 2013 (with the most likely scenario involving data security requirements added to a cybersecurity bill).

The state level is more troubling, as states continue to consider a wide range of bills on many topics. For companies operating outside of a single state's boundaries, these proposals create realistic concerns and add important transaction costs, particularly where security details or breach notification requirements are involved. It is important, however, for companies in all industries to pay attention to privacy and security bills at the state level once these bills move at all past the initial stage of bill introduction.

Key Takeaways

- If there is cybersecurity legislation, will data security and breach notification be attached?
- Will national breach notification legislation preempt all the state laws on notification?
- Watch for state legislation on ''hot topics'' that arise quickly and attract media attention.

3. International Developments

While U.S. companies struggle with the wide variety of overlapping and often conflicting requirements at the state and federal level, the international privacy and security structure presents even more complexity. More and more countries are adding their distinctive voice to the emerging cacophony of privacy and data security regulations. Global contracts that involve personal data in any meaningful way are becoming increasingly unwieldy, with more detailed and more confusing requirements and potential obligations being added regularly. The European Union continues to debate significant changes to its enormously important privacy regulation (11 PVLR 178, 1/30/12). Even though formal new requirements in the European Union will not go into effect for several years, the mere discussion of these potential changes is already causing behavioral change across the globe.

Increasingly, while lawyers and compliance professionals advise on these new changes and related developments, international privacy and security compliance is becoming an expanding challenge of simply risk management. It may not be possible (or often necessary) to meet all of the international obligations in a truly global setting. With that said, the challenge for privacy and security professionals is to meet these challenges head on, through realistic risk assessment and (hopefully) a reasoned perspective on how these requirements should be put into practice. It would be helpful for all companies involved to take a bit of a deep breath—to realize that they do not always need to make these laws and regulations appear as aggressive as possible, especially when imposing obligations on others through detailed contract requirements. On the whole, however, it is critical for companies to understand the range of new challenges and develop appropriate approaches to meeting relevant obligations, legally, contractually and operationally.

Key Takeaways

- Be careful on any contracts dealing with personal data that have international implications.
- Focus on reasonableness and risk management—it may be too hard to learn every obligation, so focus on the hard or risky steps.

  PVLR ISSN 1538-3423

- Pay closer attention to any countries that become more active on enforcement (although international enforcement remains low).

4. Regulating the Internet

Perhaps more words have been spent debating the future of privacy regulation on the internet than any other privacy-related topic. Every privacy policy change proposed by Facebook, Twitter, Instagram, or any number of other websites creates massive confusion, concern, and dismay. Congress and various regulators bemoan the changes, while others promote the value of behavioral tracking and related activities as a means of keeping the internet free and available to all. At the same time, white paper after policy paper after congressional hearing all distribute important policy pronouncements about consumer rights, overall privacy on the internet, and the risks and opportunities involving personal data, especially the hot concept of ''big data.''

The Do Not Track idea has become a focus of the debate. Promoted largely by the Federal Trade Commission and various advocacy groups, this model promises individuals increased control over their activities on the internet, in terms of protecting their paths across the internet. As with most internet restrictions proposed over the past 15 years, the devil has been in the details, and the complexity of the apparently simple proposal has threatened to overtake the debate (assuming one buys into the concern about a book buyer seeing ads about books). Now, Do Not Track—as a legislative requirement—seems destined to the same fate as most previous internet proposals. Many companies may implement their own form of Do Not Track across their systems, and public pressure may push towards modified forms of this concept. Yet, it is clear that the debate about Do Not Track and related concerns about behavioral advertising will continue to be an enormous focus of attention in 2013.

Following history, the one area where change will come will be in the area of children's information on the internet. The Children's Online Privacy Protection Act—whether you think it is strong enough or not—stands as the single most significant privacy protection that Congress has passed in its years of debating privacy on the internet. It is clear that new restrictions will come into effect in 2013 (as evidenced by the FTC's recent announcement (11 PVLR 1833, 12/24/12)). What is less clear is whether these legislative and regulatory proposals will keep pace with the ability of ''children'' (defined however you want) to engage in behavior on the internet regardless of any of these provisions, and whether the rules will be out of date even by the time they become effective.

Key Takeaways

- Be extra careful if you target your website or any particular programs or applications to children.
- Be smart about your privacy commitments—the FTC is watching promises carefully.
- Be alert to all kinds of potential consumer harm—regulatory enforcement will be broader than claims that can be made in private litigation.

5. Cloud Computing

Not all of the most significant issues to watch will involve regulation and legislation. The development of cloud computing as a new technology with enormous benefits, cost savings and potential risk clearly is outpacing the ability of the regulatory process to adapt to new technology. This means that companies need to act and make decisions now, in advance of any new regulatory developments, by adapting an old regulatory framework to a new environment. Companies in all industries are facing the direct challenge of the cloud—understanding what it really is, analyzing the potential benefits and cost savings, and trying to adapt this technology to the confusing regulatory landscape. The cloud also threatens to explode the idea of country-specific approaches to privacy and security, as well as the idea that data are located in or relate to any area in particular.

It is clear that the cloud will continue to move forward aggressively in 2013, as more companies offer cloud services and provide additional security protections for these services and additional companies seek to recognize and incorporate the potential benefits into their operating structure. The cloud will present a direct challenge to the ability of regulators to keep pace with rapidly developing technology. So far, the regulatory structure remains far behind the technological developments (although many would conclude it may be an appropriate result to allow technology to move forward in an appropriate free market way).

Key Takeaways

- Pay close attention to what cloud vendors are telling you—and don't just accept the standard language.
- Know who can access your data and generally how the data are protected.
- Have a strategy on the cloud—and make sure you're thinking about how your vendors use the cloud as well.

6. BYOD

On a more individualized level, the ''BYOD'' concept also creates significant tension between privacy and security and appropriate regulation and even good operational practice. Across the United States, individuals consistently, frequently, and increasingly, ''bring their own device'' into the workplace or use these devices to engage in communications and information exchange around the clock for an interconnected mix of personal and professional purposes. There clearly is no stopping these technological developments. At the same time, companies are faced with the challenge of trying to rein in these developments, at least to the point that the use of mobile devices does not threaten the full range of privacy and security protections that are imposed in the less mobile aspects of these companies. Again, technology and its efficiency are outpacing both regulation and operational safeguards. Some companies, despite the concerns about appearing to be luddites, are imposing strict limits, particularly in certain highly sensitive areas (such as health care). A larger range of companies—at least in the United States—are allowing these practices (or at least recognizing that they are happening with or without approval) and are simply trying to backfill their privacy and security protections. It is clear that these developments are continuing

quickly and aggressively. The challenge for every company—*repeat, every company*—is to develop an appropriate framework that permits what is going to happen anyway, and creates a structure involving both technological controls and employee training to reduce and manage the risks of these new technological opportunities. 2013 will be a year when these challenges reach the mainstream, and it will be fascinating to watch how this issue develops over the course of the year.

Key Takeaways

- There isn't a ''right or wrong'' on BYOD yet, but you need to have an approach and you need to make sure you mitigate risks based on whatever approach you choose.
- Make sure you train your people on your policy and have a means of auditing or reviewing overall compliance, especially in the early stages.

7. Overall Data Security Issues

The BYOD and cloud computing developments highlight the most significant challenge facing companies and regulators in today's environment—protecting the security of personal data (along with a wide range of other business-oriented data). While privacy issues continue to occupy the leading focus of philosophical debate, we are seeing a continuing increase in real security problems relating to data. As the world becomes more intertwined, the risks of adverse security events continue to increase. Many of these events become public; it is clear that many others do not, either because they are not disclosed or, perhaps more troubling, they are not known to the affected companies.

We will see in 2013 significant developments related to cybersecurity, an offshoot of the privacy and data security debate focused on national security and infrastructure issues. While Congress could not agree on a complete legislative package related to cybersecurity (11 PVLR 1680, 11/19/12) (and may not in 2013 either), at a minimum, we will see a significant executive order related to cybersecurity issues (*see related report in this issue*). This executive order will bring into the security discussion a wide range of industries that have not been the focus of debate relating to the security of personal information. At the same time, data security for personal information also remains incredibly important, as personal information increasingly is recognized as a valuable asset by ill-intentioned individuals, groups and even countries around the globe.

We will watch in 2013 whether Congress can agree on a framework for cybersecurity, whether (if it does) this framework includes new national legislation related to data security as well and, in any event, how companies in all industries will deal with the increasing challenges presented by the need to secure personal and proprietary data from security risks (while at the same time allowing this information to be used for appropriate purposes).

Key Takeaways

- Security reviews need to be ongoing and consistent.
- Pay close attention to where others are having problems.
- Have a strategy for keeping an eye on your largest vendors as well—that needs to be a key element of your security strategy.

8. Breaches

Despite the growth in regulatory and contractual data security requirements, there continue to be an enormous number of security breaches involving sensitive personal data, large and small, affecting virtually every kind of industry. While certain kinds of security practices have improved, this has not yet resulted in a material decrease in breaches. Presumably, the breach ''opportunities'' stemming from increased data flows and technological opportunities for mobile activity more than outweigh any specific improvement in data security practices.

Companies in all industries need to be aware that the risks of security breaches are real. This is not a philosophical debate about potential harm, such as we see with questions about the adverse consumer impact from behavioral advertising. Personal data are being lost, stolen, misused, and improperly accessed constantly by internal employees, maliciously motivated outsiders, and accidental or unintended individuals. That means that companies need to remain vigilant, need to strive continuously to improve data security practices, and need to have an efficient and effective plan to deal with security breaches quickly and responsibly.

Key Takeaways

- You will have breaches—make sure you are ready and have a plan.
- Make sure your people know where to go when there is a security problem.
- Move quickly to fix or stop problems, as many potential risks can be reduced or eliminated through quick, effective action.
- Don't let a ''no notice'' decision stop your efforts to fix problems and take corrective action.

9. Litigation

Coupled with the continuing rise in security breaches is the ongoing wave of privacy and data security litigation. Where there are reported privacy or security problems, there will be class actions filed almost instantly and essentially reflexively. There often are multiple suits, with plaintiff class action firms vying to be first in line at the courthouse.

What has distinguished privacy and data security cases to date from many other areas where class actions thrive is the lack of significant verdicts or large settlements defining monetary payments to the class of affected individuals. For more than a decade, the courts have maintained a consistent precedential line in the sand, requiring actual damage to individuals before privacy cases can proceed and damages can be awarded. That has meant that while cases continue to be filed with increasing frequency, most of these cases have found little or no success.

The big question in 2013 is whether this line in the sand will be broken at all. Plaintiffs continue to develop creative theories to avoid the substantial court precedent, and some courts appear willing to consider ap-

  PVLR ISSN 1538-3423

proaches to break from this precedent. Companies—again, in all industries—need to watch these cases carefully to ensure that this ''damages'' line remains in place. If this line were to break in any material way, we can expect to see an opening of the flood gates for a broad range of privacy and data security cases in the immediate aftermath.

Key Takeaways

- Watch for any meaningful crack in the ''no damages'' wall of precedent, particularly one that can be applied in class action settings.
- You will face private litigation if you have a large breach—but that doesn't mean you will lose the case.
- Regulators can bring cases in areas where private plaintiffs can't, because regulators can rely on broader concepts of consumer harm for their actions.

10. Enforcement

Back in 2009, many of us expected a new Obama administration to be significantly more aggressive about enforcement of various privacy and security laws. While there has been a modest uptick in enforcement to date, it has been quite limited and far less than anticipated. Will this change, beginning in 2013?

Clearly, there are significant opportunities for enforcement. The new HITECH Act rules provide for much higher penalties, along with a wider range of potential targets (once the rules are finalized and all business associates must comply). Security breaches permit numerous enforcement agencies—led by state attorneys general—to become involved in enforcement. And the Federal Trade Commission—which has focused its attention to date primarily on enormous high profile cases (e.g., Facebook (10 PVLR 1759, 12/5/11) and Google (11 PVLR 1255, 8/13/12)) or smaller but egregious situations (typically where companies have engaged in virtually no data security activities)—continues to debate internally what kinds of consumer harm should be addressed through enforcement.

Taken together, I do expect to see a continuing increase in enforcement in 2013 and beyond. It would surprise me if this growth is substantial, but I expect it to be consistent and growing. I also expect to see penalty amounts increased over the next few years, with an eye towards increased deterrence even if the volume of enforcement actions does not grow substantially.

Key Takeaways

- Take every enforcement inquiry seriously—more and more enforcement actions are resulting from what are initially limited and minor issues.
- Enforcement agencies will use a tiny opening as a way to explore a broader range of issues—be prepared any time you are providing information to an enforcement agency.
- Remember that the worst impact of privacy and security problems may be in terms of adverse publicity, as enforcement—even where it happens—often is long delayed.

Conclusion

While many of the key issues to watch for 2013 involve theoretical or potential developments, it is clear that these issues are impacting a wide range of companies even before any action is final. Global companies are putting new and more burdensome international provisions into contracts. Pressures to move into the cloud are facing every business. The BYOD debate is real and current, because of the enormous proliferation of new mobile means of communication and data exchange.

For privacy officers, compliance professionals and lawyers in the privacy and data security area, it is crucial to pay close attention to these issues and to make sure that your business—regardless of your industry—has a proactive and thorough means of staying abreast of this constantly evolving field. This will require creative thinking, an awareness of ongoing developments, a quick and thorough response to any problems, and a wide ranging approach to management of overall business operations.