Bloomberg BNA

Privacy and Security Law Report®

Privacy & Data Security for 2016

2016 promises renewed focus on privacy, data security and cybersecurity because they are no longer niche issues but core components of effectively operating a company. The author details the top ten U.S. and international developments companies must be aware of this year to better ensure an effective information security program.

The Top Ten Privacy and Security Issues Companies Need to Watch in 2016

BY KIRK J. NAHRA

Kirk J. Nahra, chairs Wiley Rein LLP's Privacy and Data Security practice in Washington, where he represents a wide variety of companies on U.S. and international issues Nahra, who is a member of the advisory board of Bloomberg BNA's Privacy & Security Law Report, is available at (202) 719-7335 or knahra@wileyrein.com. Follow him on Twitter: @kirkjnahrawork.

When I started working on privacy issues more than 15 years ago, privacy was viewed primarily as a narrow legal niche, mainly relevant for a handful of industry segments, with very little impact on most lawyers and most companies. Today, particularly in the past few years, privacy (and its cousins, data security and cybersecurity) have become regular front page news with the need for substantial attention in virtually every company. Regulators vie for jurisdiction on enforcement issues, and legislators at all levels—national, state, local and international—are looking for solutions, new requirements and overall approaches to the balance between personal interests and the potential gains for society from data.

This means that privacy, data security and cybersecurity are not in any way ''niche'' issues, but instead core components of the operating effectiveness for any company. You cannot run a meaningful company without an effective information security program. You cannot benefit appropriately from the information available to you without understanding how privacy laws and regulations impact big data and overall data analysis. And you cannot operate effectively and competitively in a global environment without adapting to the changing tides of international privacy regulation.

With unprecedented attention directed towards these topics (including the need for any company that has consumers or employees to have an effective privacy strategy), what are the key developments to be paying attention to in 2016? [1]

The Top Ten

1. ***EU Safe Harbor Resolution.*** The seismic shift in the privacy world that captured the last quarter of 2015 involved the unexpected and game-changing decision of the European Court of Justice invalidating the U.S. Safe Harbor program for data transfers to the U.S (14 PVLR 1825, 10/12/15). This decision blew up a 15 year program that provided a rational and reasonable basis to transfer personal data from the EU to the U.S. Now, following this decision (and its immediate impact), companies throughout the U.S. in all industries are scrambling to deal with the fallout from this decision.

[1] *See* Kirk J. Nahra, ''A Privacy and Data Security Checklist for All'' (Privacy in Focus, July 2015).

 ISSN 1538-3423

How this issue gets resolved will drive the privacy debate in early 2016. For many companies, the safe harbor program was the only viable option for these data transfers. Without this program, companies must address the possibility of the model contract clauses (which are impractical in many settings and may fall subject to the same weaknesses that damned the Safe Harbor program), or the even more burdensome and expensive Binding Corporate Rules approach (or certain other new options developed under the new EU data protection rules). More likely, there will be some new negotiated agreement that reduces/publicizes the limited situations that concerned the Europeans—access to personal data by the U.S. government (although passage of a disconcerting cybersecurity bill by Congress may disrupt this negotiation process) (14 PVLR 2316, 12/21/15). Until these developments occur, however, there will be dramatic uncertainty about these data transfers with real risks and substantial contractual and operational concerns for a broad range of companies across the globe.

2. ***EU Data Protection Regulation.*** While the Safe Harbor decision has generated attention and nervousness, this development has overshadowed what could ultimately be an even more significant development—the pending revisions to the overall European privacy regime through the adoption of an EU General Data Protection Regulation to replace the EU Data Protection Directive (95/46/EC) (14 PVLR 2289, 12/21/15). This broad law (expected to be finalized in early 2016 and in full force two years later) will dictate the privacy practices within Europe, with a resulting impact not only on all data transfers (remember, the initial EU directive is why the safe harbor program needed to exist) but also as core compliance obligations for EU data and thought leadership for privacy rules across the globe. Companies will need to significantly re-evaluate their overall privacy practices dealing with Europe, to accommodate new requirements related to security breaches, vendor contracts, individual consent, individual rights and a wide variety of new and different requirements. While there is a two year period before new enforcement will arise, many companies—both in and out of Europe—will need to start their planning and compliance activities *now*, to ensure that there are effective practices in place before enforcement can begin (along with the potential for dramatically increased fine amounts).

3. ***Cybersecurity.*** Cybersecurity has become the hot buzzword in the field, driven by the large number of ''cyber'' breaches and the sense that the Internet is under constant attack, from a wide variety of angles and attackers. For regulated entities, cybersecurity should not be new—it is simply a broader term that encompasses most ''data security'' requirements, and extends to a large range of technological interconnections that affect computer systems beyond just the impact on personal data. [2]

[2] For a discussion of the distinctions and overlaps between cybersecurity and data security, *see* Kirk J. Nahra, ''Mastering Cybersecurity by Learning Data Security'', Bloomberg BNA *Privacy and Security Law Report* (Sept. 9, 2013) (12 PVLR 1525, 9/9/13).

The biggest policy issue on the privacy horizon (other than the international debate on the Safe Harbor program) involves the question of whether ''big data'' needs new or different regulation.

Companies in every industry face challenges from cybersecurity threats, even those that have no meaningful consumer personal data. For some industries, including many of those identified by the government as ''critical infrastructure'' industry (e.g., chemical, utilities, transportation), these risks involve public threats when systems do not work effectively. For companies facing privacy and data security threats as well (most consumer oriented industries and large employers), cybersecurity should be a point of additional emphasis, focusing attention on controlling these risks, identifying ongoing weaknesses and taking effective steps to prepare for events that are increasingly likely to happen.

4. ***Big Data.*** The biggest policy issue on the privacy horizon (other than the international debate on the Safe Harbor program) involves the question of whether ''big data'' needs new or different regulation. The big data phenomenon, sometimes referred to as the Internet of things (IoTs), actually refers to two related but different issues. Big data is primarily a technological issue, the ability to gather, store and analyze enormous volumes of data. The IoTs is a related issue that involves an extraordinary number of new data sources never thought possible, which supplements and complements the ability of big data to conduct effective analysis of these new data sources (obviously combined with the existing volumes and sources of data).

Companies in every industry face challenges from cybersecurity threats, even those that have no meaningful consumer personal data.

The technology of big data and the IoTs is growing on a daily basis. Our policy debate on this has not moved forward much in the past few years, nor is there any realistic likelihood that this will change soon. Accordingly, for a growing range of companies (essentially, traditional personal data companies plus the new sources not previously thought of as privacy concerns—such as car companies and various electronic products) the questions become economic, operational, public relations and ethics. The White House in its big data report raised many concerns about how this data can be used. Companies need to be evaluating what data they are gathering and how they are using it. They need to pay more attention to their downstream vendors and partners, who can capitalize on data more than ever before. And companies need to think about the increasingly important issue of trust from consumers and oth-

  PVLR ISSN 1538-3423

ers, about how their data is being used and what commitments are being made about this data.

5. ***Research.*** With ''Big Data'' comes the opportunity for many new things, including additional avenues for research. At the same time, current rules (including but not limited to those in the health-care industry) are viewed as creating barriers to some kinds of effective research, and it is clear—at a minimum—that the rules and operating procedures are complicated and confusing enough that certain research efforts are being impeded. Pending legislation in Congress (the 21st Century Cures Act), which already has passed the House, purports to free up health-care data for additional research opportunities, but the current privacy provisions have received little attention in the much broader overall scope of the bill, and likely will create meaningful privacy risks if not modified (14 PVLR 1324, 7/20/15).

In addition, there is a current rulemaking proposal to revise the ''Common Rule,'' the primary set of research regulations related to federal funded ''human subjects'' research, with a goal of streamlining research requirements where there are not meaningful privacy or other risks to research subjects (14 PVLR 1615, 9/7/15). Research is not just for universities, and companies in a wide variety of industries need to understand these research rules (including when their own internal data analytics ''cross the line'' into the regulated research area), and an even larger group of companies have data that can (and should) be made available for beneficial research projects.

6. ***De-Identification.*** The big data phenomenon also points to a related issue that presents the possibility of balancing the risks and benefits of big data—the idea of de-identification, or removing identifiers such that the concerns about privacy are removed or reduced in ways that make the data still useful without creating meaningful privacy risks. De-identification has been a source of enormous and confusing debate. Governments discuss de-identification at the threshold of the privacy debate, in connection with how personal data is defined. Technologists and data scientists debate the potential for re-identification of data subjects in various scenarios, and the media (typically without thoughtful analysis) reports every potential re-identification as a fact that threatens privacy.

It is clear that the de-identification debate is complicated, but it is also clear that there are certain core elements. First, de-identification presents a potential win-win scenario, where privacy risks are reduced in dramatic ways, while the value of data largely remains. It is also clear that there is an immediate trade off of sorts between privacy and data value, with reduced privacy concern often meaning less valuable, useful or reliable data. So, as the volume of data grows, and the potential public and private benefits of this data grow even more, it will be critical for there to be responsible and thoughtful debate about de-identification, so that the value of data can be preserved and improved at the same time that privacy can be protected.

This also needs to encompass the debate (largely for public entities) about transparency, where true public disclosure of data creates the most substantial privacy concerns. In other environments, where transparency is a secondary value, these risks often can be controlled through legal, contractual and security protections, to preserve data benefits without meaningful privacy risk. Managing an effective de-identification process—whether in individual industry segments like healthcare or on a broader basis where the rules are more ambiguous—presents both a challenge and opportunity for many companies seeking to capitalize on the value of their data.

7. ***Wearables/Non-HIPAAHealth-Care Data.*** The clear limitations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule's scope have been exposed through the development of broad new range of sources for health-care data that are outside the scope of the HIPAA rules. Often referred to as ''wearables,'' these new sources actually include a wide variety of sources, including wearables, health-care mobile applications, health-care websites and others. We have reached (and passed) a tipping point on this issue, such that there is enormous concern about how this ''non- HIPAA'' health-care data are being addressed, and how the privacy interests of individuals are being protected (if at all) for this ''non-HIPAA'' health-care data (14 PVLR 2033, 11/9/15).

This issue will continue to be the source of extensive debate in 2016, as a broad range of regulators, legislators and privacy advocates seek solutions on filling this widening gap. At the same time, businesses need to consider the policy, business and ethical implications of their activities where they are collecting sensitive health-care data perhaps outside of current regulations. It will be critical to plan on this issue, to address where the law stands today (both where data practices are and are not regulated), and to evaluate where the law will be going along with public perception of what appropriate practices should be. These data exist, are growing, are valuable, and the legal system is struggling to catch up, once again.

For the FTC, therefore, 2016 will be a key year. Will its overall authority be confirmed in the courts, giving the FTC more room to take broad action in these areas?

8. ***FTC Enforcement.*** For more than decade, the Federal Trade Commission (FTC) has been both the most aggressive privacy and data security regulator in the U.S., but also the regulator with the broadest reach and the largest impact on the perceptions of privacy and security regulation for the U.S. In 2016 (as with 2015), the FTC faces substantial ongoing challenges to its enforcement authority that could dramatically reshape the enforcement landscape across the country.

After more than a decade of largely unfettered authority to enforce data security practices, the FTC faced two major challenges in 2015. In the first, the *Wyndham* litigation, the FTC fended off a core challenge to its basic authority on data security, and has now settled litigation and enforcement with Wyndham Worldwide Corp. without any limitation on its overall authority (14 PVLR 1592, 9/7/15). Wyndham challenged the FTC's ability to enforce any data security standards, claiming that it had no statutory authority on these issues and no clear standards to subject companies to enforcement. The U.S. Court of Appeals for the Third Circuit upheld

the FTC's authority, but this decision is unlikely to be the last word on this topic, as other defendants may take up Wyndham's challenge.

The *Wyndham* decision surprised few people. The second key decision involving LabMd Inc. presented the same issue as the *Wyndham* case, but also the separate question of whether the FTC could use its general data protection authority to take action against a HIPAA covered entity (14 PVLR 2109, 11/23/15). In a major surprise, at the administrative level within the FTC, the judge resolved the LabMdchallenge for the time being on an entirely new issue—whether the FTC needed to allege reasonable harm from a data security threat before it could take action. This surprising result will be challenged on appeal within the FTC's administrative process, but it is clear that this decision and the resulting impact (which addressed neither of the two key issues initially presented) is not yet complete.

For the FTC, therefore, 2016 will be a key year. Will its overall authority be confirmed in the courts, giving the FTC more room to take broad action in these areas? If so, will the FTC look to develop a similar common law for data privacy? Or will the *LabMd* case restrict this scope in new ways, with subsequent attacks, on the other pillars of FTC authority? And, if the FTC's abilities are curtailed, will Congress finally take action on data security (since the Third Circuit's *Wyndham* decision gave Congress an intermediate reprieve from the need to pass a law in this area). In addition, as more government agencies enter the privacy enforcement field, how will the FTC interact with these other regulators in acting against companies facing privacy and security problems? [3] (14 PVLR 2245, 12/14/15).

While breaches affecting personal data will likely continue to grow, they have become almost normalized. Will there be a "cyber" breach that has a broader impact on a large segment of the economy or impacts beyond personal data?

9. ***Data Breach Litigation.*** While risks of enforcement dominate many of the internal conversations at private companies, the threat of private litigation following a data breach is much more likely than enforcement. These claims—often with multiple competing and overlapping classes—are becoming a normal and expected effect from a data breach, where plaintiffs' lawyer jump onto breaches almost instantly, and wait for the facts to develop later. To date, most of these cases have been unsuccessful. Courts have built a strong wall of precedent holding that a realistic threat of actual injury is necessary before a case can even proceed, before addressing the other claims that make class action litigation complicated and challenging. Nonetheless class actions continue to be brought in increasing numbers for many large scale data breaches.

The class action bar continues to be creative in inventing theories for these cases, and, repackaging common law claims and certain statutory claims that seldom see the light of day outside of law school textbooks. In 2016, we will see continued efforts to chip away at the existing wall of precedent. For example, in the Supreme Court, the justices will address the *Spokeo* case which may expand the kinds of "injury" that can be claimed by plaintiffs (14 PVLR 2039, 11/9/15). In other cases, there have been small gaps opened that lawyers will attempt to expand. For any company facing a data breach, these lawsuits will continue to at least be a substantial nuisance and, if some start falling the other way, could become a major problem.

10. ***Privacy/Security Wild Card.*** Earlier this year, no one thought that the biggest privacy issue of the year would be the destruction of the EU/U.S. Safe Harbor. Instead, the unprecedented Anthem breach—one of the largest of its kind—occupied our early attention (14 PVLR 227, 2/9/15), followed quickly by the confusing and threatening Office of Personnel Management breach affecting the U.S. government (14 PVLR 1031, 6/8/15). So, what's the wild card we need to be thinking about into 2016?

Clearly, security breaches dominate our attention in a variety of settings. While breaches affecting personal data have grown—and likely will continue—these have become almost normalized. Will there be a "cyber" breach that has a broader impact on some large segment of the economy or other impacts beyond personal data? Will some combination of breaches lead Congress to finally pass a broader security bill? Will potential abuses in currently unregulated areas (wearables or other aspects of the IoTs), or some breach that directly affects members of Congress—finally lead to a broader national data privacy bill in the U.S.?

Conclusion

In any event, companies need to be watching these developments, planning their strategy, thinking about their vendors and their business partners and how they work with data on a regular basis. The message is clear—the full package of privacy and security issues must occupy the attention of every company, at a senior management level. This is a core strategy issue for many companies—across a far broader range of industries than thought previously—and constitutes an element of managing and operating most businesses today.

Companies need to be thinking about these issues regularly—not solely because of compliance obligations but because of the direct and substantial impact on businesses in the operation of core business activities.

[3] For a broader discussion of this "multi-agency" issue, *see* "Views on Privacy and Data Security Enforcement From Kirk Nahra, Partner, Wiley Rein LLP," Bloomberg BNA *Privacy and Security Law Report* (Dec. 14, 2015).

  PVLR ISSN 1538-3423