Bloomberg Law®

Privacy and Security Law Report®

Data Security

The Top Ten Privacy and Data Security Developments to Watch in 2018

Privacy in 2018

As privacy and data security issues increasingly continue to permeate almost all activities of all companies, the author details the top-10 U.S. and international developments in 2018 that companies must be aware of to better ensure an effective information security program.

BY KIRK NAHRA

Sex toys are now tracking personal data, and sharing this data both across geographic borders and for (allegedly) undisclosed purposes. A Canadian company recently settled a class action relating to privacy claims involving ''adult sensual lifestyle products'' that transmitted various customer utilization data. Even the disclosed purposes for the data collection involved, apparently, ''product improvement.'' As one reporter covering the settlement indicated ''think twice about connecting those sex toys to the Internet.'' Roberts, Jeff John, ''Sex Toy Maker Pays $3.75 million to settle 'Smart' Vibrator Lawsuit,'' Fortune (March 10, 2017).

Now that I have your attention, it is clear that privacy and data security has moved from an issue impacting primarily healthcare and financial services companies, to an issue that affects, in large and small ways, virtually every company across the globe. These issues affect litigation, mergers and acquisitions, product development, research, corporate strategy, business partnerships, and, in some way most activities of most companies. Data is everywhere. And this data is increasingly personal—or at least tied to individuals—and is being examined for its utility in a broad range of areas, many of which were unheard of a decade ago. We are drawing links in activities using this data to generate insights in areas that we have never before thought of as linked. And with these opportunities comes as well a broad range of compliance, enforcement and business challenges for companies, and new risks (along with at least some benefits) for individuals across the globe.

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 is available at (202) 719-7335 or knahra@wileyrein.com. Follow him on Twitter: @kirkjnahrawork.

Thirty years ago, privacy law generally did not exist. Virtually no one at a law firm or company worked on privacy law issues. Ten or fifteen years ago, the area began to grow, as a specialty niche in a handful of industry sectors such as health care and financial services. Now, privacy law has become a key foundational knowledge base for many lawyers, and drives full-time employment for a wide array of consultants, compliance officers, data analytics personnel, product engineers, customer service representatives, marketing executives and corporate strategists. The International Association of Privacy Professionals has grown from several hundred people to more than 34,000 members, across the world. It is increasingly challenging—even for privacy professionals—to master all aspects of privacy law and practice. With that in mind, what are the main developments to pay attention to in 2018?

GDPR The imminent arrival of the European Union's new General Data Protection Regulation in May 2018 is clearly the dominant privacy story of the year. A recent study by the International Association of Privacy Professionals (with Ernst & Young) indicates that the Fortune's Global 500 will spend roughly 7.8 billion to

 ISSN 1538-3423

implement GDPR. IAPP also estimates that the GDPR's global reach will require the hiring of at least 75,000 data protection officers worldwide.

The GDPR—expanding and updating the existing EU privacy directive—creates new privacy and data security obligations not only for virtually every company operating in the EU but also a broad variety of other entities around the world. The GDPR creates obligations for both data controllers and data processors. All personal data is covered. New data security obligations and breach notification requirements are imposed. The new ''right to be forgotten'' needs to be implemented. And the GDPR requires a new array of obligations in connection with anonymous and pseudonymous personal data. The GDPR creates the possibility of enormous fines—up to 20,000,000 euros ($24.12 million) or (in some situations) 4 percent of global turnover, whichever is higher. In addition, the GDPR leads to needs for new privacy leadership within many companies, the need to revise and expand tens of thousands of contracts, improved security protocols, new breach notification templates and a broad variety of overall privacy controls. In addition, much like the EU Data Protection Directive, which guided privacy thinking in most countries around the world, the GDPR system likely will motivate more countries to expand their data protection regimes.

Privacy Shield and Other Data Transfer Obligations The GDPR also highlights the need for effective international data transfer mechanisms. After the sudden demise of the U.S.-EU Safe Harbor program, the U.S. government and its EU counterparts developed the EU-U.S. Privacy Shield program, a new and improved version of the longstanding Safe Harbor program, to address the concerns raised about Safe Harbor and the impact of the EU court decision striking down the program. While hundreds of companies have moved to implement Privacy Shield, the long-term viability of the program remains unclear. There are both pending court challenges, new potential bases for review after the GDPR is fully implemented and the ongoing concern that some activities of the current administration may raise the concerns of EU regulators. While the program ''passed'' its first annual review from the EU leadership, there remain significant potential issues with the program. The EU concluded that ''On the whole, the report shows that the Privacy Shield continues to ensure an adequate level of data protection. However, there is room for improvement.''

At the same time, the model contract clauses—another currently viable vehicle for data transfer from the EU to the U.S.—also is subject to ongoing court challenges that may reduce or eliminate its viability. Given the recognized importance of data transfer needs, it is critical for companies to stay on top of these constant developments and for multiple governments to work cooperatively to permit reasonable data transfer vehicles while still appropriately protecting individual privacy.

Other Non-EU Data Transfer Programs Despite the prominence of the privacy shield program, it applies only to EU-US data transfers. There is a separate (although similar) program governing Switzerland. And there are open issues about the implications of Brexit on transfers from the U.K.

And then there is the rest of the world.

For the past few years, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System has been gaining momentum both in terms of the number of countries that have joined and the number of industry associations and companies supporting the initiative. The system was designed to facilitate cross border data flows and raise the level of privacy protection for consumers in the APEC region. Currently, six countries (Canada, Mexico, Japan, the U.S., South Korea, and Singapore) are participating or in process of joining the system, and two more (the Philippines and Chinese Taipei) have noted their interest in joining in 2018 and beyond. In addition, the Australian Attorney-General's Department recently announced that it would move forward with an application to participate in the APEC CBPR system, and that it will work with the Office of the Australian Information Commissioner and businesses to implement the CBPR system requirements. All told, these countries represent almost half of the APEC region. With the expected growth of the CBPR System over the next few years, it is possible that more than 1 billion people will be covered by the transfer mechanism in 2020, accounting for participation of nearly every APEC economy. In addition, a team is exploring whether the CBPR System—a voluntary but enforceable privacy regime—could be considered as a certification mechanism that would be recognized as compliant with the EU's GDPR. Interoperability between regional privacy regimes is a key priority for many businesses.

Meanwhile, various non-APEC economies have expressed an interest in learning more about the APEC CBPR System as a code of conduct mechanism for privacy program compliance and cross-border data flows. The APEC CBPR System was designed to provide significant benefits for participants—it is scalable, flexible, built on internationally-recognized privacy practices, enforceable, and effective. So, one development to watch going forward is whether the CBPR system, or the GDPR Privacy Shield program, or some other variation, will become a ''common language'' for international data transfers.

Cybersecurity While data security requirements have been in place for more than a decade (including the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, the Gramm-Leach-Bliley Safeguards Rule and the enforcement activities on reasonable and appropriate data security from the Federal Trade Commission), cybersecurity is a new(ish) buzzword that has captured significant new attention. The overlaps between ''data security'' and cybersecurity are complicated and confusing. *See* Nahra, ''The Tensions and Overlaps Between Cyber and Data Security,'' (July 2013). Simply put, data security tends to refer to protections involving personal data. Cybersecurity tends to involve system interconnections and concerns about the overall internet operations along with various national security concerns. Data security tends to be regulated and subject to enforcement. Cybersecurity involves guidelines, information sharing, potential national security implications and a general fear about ''taking down'' or ''taking over'' a company's electronic infrastructure.

Congress and the Administration are reviewing various voluntary programs, along with information, education and best practices. Other entities—primarily Na-

  PVLR ISSN 1538-3423

tional Institute of Standards and Technology (NIST), which continues to update its cybersecurity framework—are creating cybersecurity best practices and general industry guidelines. In any event, as we continue to read about larger and more extensive cybersecurity breaches on a mind numbingly regular basis, companies—in every industry, regardless of their role in personal data—must pay close attention to an almost constant vigilance about effective protection of electronic assets and ongoing monitoring and mitigation of significant cybersecurity risks.

Breach Litigation Because of the constant array of large and small security breaches—triggered by causes ranging from insider malfeasance or negligence to ''sophisticated'' hacker attacks and the loss of every conceivable electronic and paper media—we are seeing a substantial growth in both the speed and volume of breach related litigation. The key issue in this litigation remains essentially the same—across the broad variety of defendants and breach situations: did the plaintiffs suffer an ''injury'' such that the plaintiffs—in a class or not—have standing to pursue damages in the litigation. The U.S. Supreme Court has danced around this issue, in several recent cases touching somewhat indirectly on this point. Cases presenting this issue directly—including a pending petition in the CareFirst Inc. case—are moving slowly towards the court.

In the meantime, the plaintiff's bar is becoming increasingly creative and aggressive, with some cases being pled almost instantaneously with the announcement of a breach. While the defendants continue to win significantly more cases than they lose, there are increasing chips in the wall of precedent. Until we see a definitive answer on the harm standard, breach litigation will become a necessary cost of doing business after a breach. If there is an expansion of what is considered injury in these cases, then this relatively modest litigation cost will become a massive expenditure across the board for companies with breaches, since the true benefit to defendants of the harm threshold to date has been the ability to cut off litigation at the pleading stage usually before expensive discovery. At that point, we will then move to all of the ''second level'' issues in this litigation—class certification, causation, proof of damages (beyond the mere allegation of damages for pleading purposes), and the like. Those of us involved in breach-related litigation will be working on these issues for many years to come. Those who are potential defendants should use this uncertainty as an incentive to beef up security practices—to reduce the likelihood of a breach in the first place. Moreover, while effective mitigation may not impact the standing issue in litigation (since mitigation steps have seemed to have no impact whatsoever on whether a case is filed), those steps will reduce the likelihood of a significant ultimate outcome on damages and any potential regulatory proceedings.

FTC Enforcement The Federal Trade Commission remains the agency with the broadest scope for potential privacy and security enforcement as well as the most extensive track record on these cases. Despite that history, the future of FTC enforcement is wildly uncertain. On the one hand, there are ongoing challenges to the FTC's authority—particularly through the longstanding and increasingly complicated LabMD case. The potential outcomes to these challenges range from a complete endorsement of the FTC's approach, to a dismantling of this approach to a meaningful reduction in FTC authority (if more precise individual harm becomes a required first step of any enforcement activity). In addition, as with many other areas of federal government enforcement, there is a substantial question as to whether the FTC will in fact pursue ongoing enforcement related to data security and/or privacy. The FTC leadership is still being completed, and there are hints from interim commissioners that there may be an enhanced focus on consumer harm before any enforcement action is taken.

OCR Generally For the health-care industry, the primary regulator remains the Office for Civil Rights. While enforcement from OCR has been steadily rising in recent years, OCR remains an effective, thoughtful and reasonable regulator, one who balances compliance efforts with an understanding of industry practice, a realization that ''too aggressive'' enforcement may reduce appropriate information sharing to the detriment of patients and an ability to evaluate when covered entities are trying to do the right thing.

It is clear that enforcement has slowed this year. Whether that is due to ''typical'' leadership transition in a new administration or something else is much less clear. The recent departure of Deven McGraw from her role at OCR also threatens to adversely affect both patients (through her thoughtful leadership on privacy issues) and the industry (given her knowledge of industry practice and ability to balance compliance with a real world approach). *See* Nahra, ''An Appreciation,'' *Privacy in Focus* (November 2017). While there is highly competent career staff remaining, there is little useful information at this point about any new approach of the new administration in this area. OCR also is beginning to confront the enormous challenges that will result from investigations related to business associates, the service providers for the health care industry, which range from solo practitioners to the biggest companies in the world, with everything in between, and an enormous variation in the roles played with protected health information and the volume of such information. While it is unlikely that there will be a significant change in overall enforcement approach, we may see much less enforcement due to staffing changes and budget reductions. It will be critical to watch any new appointments at the office and to see if enforcement returns to recent levels in 2018.

The Role of the States Whether or not the federal government significantly cuts back on its privacy and security enforcement efforts, all companies should expect that state enforcement efforts will grow in 2018 and beyond. The states have always had a role in privacy enforcement (with authority that loosely mirrors in many states the general authority and jurisdiction of the Federal Trade Commission). While many of us have expected a broader role in general from the states, this has been somewhat slow in coming. Now, we can expect to see two major areas for the states going forward. First, the states will step in where they see a failure of the federal government to act, on a specific case or in a particular area. Equifax, for example, has been hit with a 50 state complaint based on its recent security incident. The California Attorney General recently announced a $2 million settlement with Cottage Health System, which agreed to a $2 million settlement to resolve allegations that Cottage failed to implement ''ba-

sic, reasonable safeguards to protect patient medical information.''

We also can expect to see states jumping into gaps in the privacy regulatory structure. For example, in early 2017, the New York Attorney general announced settlements with three entities at the same time (as described in the AG press release):

- Cardiio, an American company that sells Cardiio, an app downloaded hundreds of thousands of times that claims to measure heart rate.
- Runtastic, an Austria-based company that sells Runtastic, an app that purports to measure heart rate and cardiovascular performance under stress.
- Matis, an Israel-based company that sells My Baby's Beat, an app downloaded hundreds of thousands of times, which Matis previously claimed could turn any smartphone into a fetal heart monitor, despite the fact that it has never been approved by the U.S. Food and Drug Administration (FDA).

While each settlement was based on its own facts, the AG's office focused on three separate areas of concern. First, the AG was concerned about the accuracy of various health claims made by the apps. The developers generally agreed to provide additional information about testing of the apps and to change their ads to make them non-misleading. Second, because these apps are not regulated by the FDA, the settlement required the apps to post clear and prominent disclaimers informing consumers that the apps are not medical devices and are not approved by the FDA. Third, on the privacy front, the settlements required specific changes to privacy policies and practices. The app developers are now required to obtain affirmative consent to their privacy policies for these apps and disclose that they collect and share information that may be personally identifying (including users' GPS location, unique device identifier, and ''de-identified'' data that third parties may be able to use to re-identify specific users).

Companies operating in relatively unregulated spaces should expect to see more activity from the state attorneys general in the years ahead (in addition to a likely increase in enforcement actions related to state breach notification laws, likely driven by Uber's failure to report its large breach).

States also will continue to be (and perhaps will grow in importance) as legislative innovators on privacy issues. While California has been the primary ''thought leader'' on privacy issues, we can expect to see states in a broader range of areas moving into new legislative proposals, whether biometric laws (like in Illinois), expanded data breach notification laws or in a broad variety of other areas where there are gaps that exist that are not being filled by the federal government.

IoT Issues and Unregulated Data Our sex toy example, along with these New York cases, drive home one of the biggest privacy and security developments of the past years—the expansion of the internet of things IoT), and the creation, disclosure, maintenance, and analytics of data coming from an ever-growing range of sources, most of them essentially unheard of a decade ago. Privacy and data security issues are now critical beyond traditional ''privacy related'' industries and now include toy manufacturers, car companies, alarm systems, refrigerators, thermostats, and a host of other products and services where personal data is being collected simply because the data now exists. Data scientists and analytics professionals may not yet know how this information is valuable, but they are gathering as much as they can in an effort to analyze and profit from this data.

These developments raise a variety of issues for companies in this broad range of industries to consider. For the most part—at least in the U.S.—this data is largely unregulated. ''Unregulated'' in this context means that there is no specific law or regulation governing how this data is used or collected. Obviously, companies in these areas do still need to consider the requirements of the Federal Trade Commission and state attorneys general, through their general consumer protection oversight. But, this means that the ''rules'' governing this data are, at best, vague, and companies have significant leeway in how they gather and use this data.

These challenges arise in any industry where IoT data is being collected. The issue may be particularly acute in the health care field, where the sources of health care data (and data that is not obviously health care data but is proving useful for healthcare purposes) is being collected across web sites, mobile applications, wearables and a plethora of sources not constrained by the existing HIPAA rules. The challenges—for both industry and consumers—are growing every day because of the overlaps and gaps in the rules and ongoing confusion about the sources of this data, particularly as it moves from place to place. For a discussion of potential ''solutions'' to this issue in the health care industry, *see* Nahra, ''Moving Toward a New Health Care Privacy Paradigm,'' *Privacy in Focus* (November 2014).

The Obama Administration, through various efforts, had been investing heavily in analysis and assessments of the risks of this ''big data environment, where data was emerging from these new sources. Their efforts had led to thoughtful consideration of both the risks and benefits of this new kind of analytics, and was moving, slowly but steadily to potential legislative or regulatory proposals. These efforts seem to have stopped entirely under the new administration. Therefore, while the regulatory efforts have stopped, the movements towards the creation of this data are moving even faster. That leaves, essentially, an ethical and risk management component that needs to be considered by any company gathering and utilizing this data. What are the realistic rules? How will these efforts be perceived, by my customers, consumers, business partners or others? What could go wrong with my collection of this data? And, perhaps most significantly, how will the plaintiffs' attorneys—who are unconstrained by regulatory considerations—look at my data collection efforts?

My concern is that companies may view this unregulated environment as a free pass on data collection. Clearly, this is not the case outside of the U.S. But, even within the U.S. it is critical for companies and their data protection lawyers, compliance professionals and risk management advisors—to carefully consider and understand how personal data is being collected and used by the company (including where this data is being disclosed), to permit an overall effective analysis of the appropriate best practices in this new and potentially unrestricted but still risky environment.

Other Legislation This unregulated environment—and a variety of other significant developments involving data security, security breaches and the like—have led to the question of whether the Congress is capable

   ISSN 1538-3423

of or willing to pass legislation to address these issues. For the past several years, for example, there has been at least one ''massive'' security breach that has led commentators to say that the tipping point was finally here on data breach legislation. We have (so far) been wrong each time. Will the Equifax Inc. breach change this, where the Anthem Inc., or Sony Corp., or Target Corp., or Office of Personnel Management breach did not? What about the various bills designed to dictate specific data security practices for companies across the board (essentially turning the FTC's ad hoc enforcement authority into actual law)?

The areas of data breach notification and data security at least had moved to actual proposed legislation. What about the IoT or other ''gap filling ''privacy legislation? Those issues had not yet arisen, even under more favorable Congresses. So, we will continue to watch, as specific events lead to specific proposals, but it is hard to bet heavily on the likelihood of meaningful privacy or data security legislation in the upcoming year.

Conclusions Collectively, the growing global privacy and security community will need to address some increasingly complicated issues in the next year. There are both formal issues—mainly GDPR implementation and the related data transfer rules for the EU and globally—and practical or operational issues involving emerging best practices for new data and new technology. We are facing—at least in the U.S.—the meaningful likelihood of reduced enforcement (whether through intent or budget reductions) and the related need for data professionals to become effective stewards of company data, with appropriate consideration of individual privacy and appropriate business goals. At the same time, as more and more companies must grapple with the need to manage individual data, companies across a broad range of industries also must deal with the increasing array of legislative and regulatory overlaps—across industry, practice or country lines, leading to the need for increasingly sophisticated privacy advice. In addition, with cybersecurity as a constant concern and security breaches arising in frustratingly large numbers, the need for effective integration of privacy and security controls is increasingly important—with the need for both technical and legal/compliance support for these activities. While the area of privacy and data security law is a relatively new field, there is no indication whatsoever that the growth in obligations and responsibilities is slowing down in any way.

BY KIRK NAHRA

To contact the editor responsible for this story: Donald Aplin at daplin@bloomberglaw.com