Privacy and Cybersecurity Top 10 for 2018

This past year was marked by ever more significant data breaches, growing cybersecurity regulatory requirements at the state and federal levels and continued challenges in harmonizing international privacy and cybersecurity regulations. We expect each of these trends to continue in 2018.

As we begin this New Year, here is list of the top 10 privacy and cybersecurity issues for 2018:

1. **EU GDPR**

The May 25, 2018 effective date for the EU’s General Data Protection Regulation (GDPR) will no doubt be a central focus of 2018. Europe’s omnibus new framework for data protection law applies to (almost) all entities that collect and process EU personal data regardless of where the data are processed. The GDPR expands the rights of EU individuals and the obligations placed on organizations. Companies around the world will also be watching how EU data protection authorities staff up, interpret the new GDPR and respond to the inevitable court challenges that will follow.

A key component of the GDPR to watch is how the EU regulators use their new penalty regime. Entities found to be in breach of GDPR could be fined up to 4 percent of annual global turnover or €20 Million (whichever is greater). Smaller infringements, such as an organization’s failure to have their records in order, could result in fines of up to 2 percent of annual global turnover or €10 million (whichever is greater). Whether the EU regulators will have the resources to launch, investigate and prosecute such significant enforcement actions remains to be seen – along with the degree of consistency, transparency, reasonableness and due process that the regulators bring to bear.

2. **Data breach litigation risks**

Data breach litigation may reach a turning point in 2018. Until recently, “standing” to sue has doomed most data breach complaints due to significant uncertainty about whether the data breach plaintiffs had suffered sufficiently serious and certain injury. At present, litigation of this type has typically failed at the pleadings stage due to plaintiffs’ failure to demonstrate the “injury in fact” necessary for Article III standing. Plaintiffs commonly struggle to articulate damages that are not purely abstract. They can only allege that a company experienced an incident, but not necessarily that the affected individuals suffered concrete and particularized harms. However, in some recent cases in the Seventh Circuit, Ninth Circuit, D.C. Circuit and elsewhere, data breach plaintiffs have survived motions to dismiss on standing grounds based on the risk of future harm.
While the hurdles remain high for plaintiffs, companies suffering data breaches may face an increasing risk of discovery and civil liability. As cases work their way through the federal and state systems, one of the major stories of 2018 may be whether a consensus emerges regarding legal theories and liability for companies that suffer data breaches. While most data breach cases have tended to involve tort or contract theories, to the extent that future litigation turns on statutory claims, the import of the Supreme Court’s ambiguous standing decision in *Spokeo, Inc. v. Robins* will certainly be back in play.

3. Supreme Court Developments

In November 2017, the Supreme Court heard oral arguments in *Carpenter v. United States*, a case that could have wide-ranging effects on the meaning of privacy and the ability to collect records of citizens’ location. The decision could also potentially re-work the seminal third-party doctrine that denies individuals’ reasonable expectation of privacy (under the Fourth Amendment) in data turned over to third parties (like bank account records or telephone billing records). In *Carpenter*, the government obtained months’ worth of a suspect’s cell phone location records pursuant to the Stored Communications Act (SCA). Instead of a search warrant, the government relied on an order under the SCA based on a standard lower than “probable cause,” namely that “specific and articulable facts show that there are reasonable grounds to believe” that the telecommunications records sought “are relevant and material to an ongoing criminal investigation.” *Carpenter* argues that the government is required to receive a warrant under the Fourth Amendment for his location records. This case is expected to decide whether law enforcement agencies may obtain cellphone data from third-party service providers without a warrant, and it may shed light on how the Court now views the longstanding third-party doctrine that holds an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. If so, the case may have wide repercussions on the meaning of privacy, the sensitivity of location data and the requirements for corporations (and others) that collect and process geolocation information.

There is also another sleeper case with potential for notable privacy rights impact. In *Byrd v. USA*, the Supreme Court will address whether a form car rental agreement can vitiate a driver’s Fourth Amendment expectation of privacy. In *Byrd*, a police traffic-stop search revealed that a rental car had 49 bricks of heroin in the car’s trunk. Normally, a car’s driver would have a reasonable expectation of privacy in the contents of the vehicle, but the rental agreement here did not list the driver, and the driver was thus not legally entitled to drive the car. The Third Circuit recognized that a circuit split as to “whether the sole occupant of a rental vehicle has a Fourth Amendment expectation of privacy when that occupant is not named in the rental agreement.” The Supreme Court will confront whether such a driver does have a constitutional right to privacy and can challenge the validity of the search of the vehicle regardless of the terms of the contract, although it may go further and explain how contractual terms affect broader commercial privacy expectations.

Other cases on the Supreme Court’s docket may also help resolve the persistent tensions raised by the requests of U.S. enforcement for data that is stored overseas or involves non-U.S. persons. These cases have been a central part of post-9/11 privacy law. Significantly, though, the U.S. Supreme Court may not be the only high court to require the attention of global privacy mavens, as the EU’s courts will surely contribute substantially to the dialogue.
4. Litigation in the European Court of Justice

The Court of Justice of the European Union (CJEU) has already proved that it can alter the EU-U.S. dialogue with its stunning abrogation of 15 years of practice under the EU-U.S. Safe Harbor. In 2018, we could see how the CJEU applies fundamental right protections to international data transfers when it considers model clauses and how they may be used to transfer data internationally, particularly under the potentially more rigorous GDPR enforcement regime. The General Court of the EU is now considering the validity of the Privacy Shield in a case brought by La Quadrature du Net and others (with a second case brought by Digital Rights Ireland being dismissed for lack of standing in November 2017). U.S. companies are intervening, now that their ability to transfer data out of Europe is being threatened. This year could see the CJEU’s decision on the Privacy Shield for transfer data to the United States and perhaps even on the model clauses, although ultimate decisions on the merits may easily reach into 2019 or beyond.

5. The Relentless Rise of Big Data and AI

The era of artificial intelligence processing previously impossibly large databases has already begun. As big data and AI make our lives easier and more of our quotidian activities are pushed online, cybersecurity and privacy issues will continue to be business enablers or business roadblocks. Some of the big data stories from this year include the success of Alpha Zero, a software that has taught itself to play games, beating the world’s human and computer masters at Go and chess. AI is also fast becoming a central player in cybersecurity efforts, as machine learning can help detect insider threats and help networks protect themselves better and faster. And the robot Sophia, which can communicate with realistic facial expressions and process emotional data, was granted citizenship in Saudi Arabia, raising issues of the legal status of AI.

Indeed, autonomous vehicles and robotics will spawn increasing legal and social questions, likely prompting businesses and governments to consider how to address effects of these technologies. For example, states continued to enact legislation concerning autonomous vehicles, and the latter half of 2017 saw the introduction or consideration of three separate pieces of AI-related legislation: the “SELF DRIVE Act,” which addresses the safety of automated vehicles; the “AV START Act,” which was introduced by a bipartisan group of Senators to similarly tackle driverless cars; and the “FUTURE of AI Act,” introduced by a bipartisan group of Senators to create an advisory committee on AI issues. We anticipate this legislative interest to remain and potentially grow as these technologies continue to develop.

6. The Internet of Bodies

Perhaps the most personal aspects of cyberspace will arise with the marked increase in the rise of wearables, digital pharmaceuticals and advances in personal medicine. Pills can tell an app when they have been taken, and heart monitors can alert your doctor if you’re having a heart attack. As apps let you determine blood pressure, walk you through pregnancies and interact with body implants, watch for a rise of privacy concerns, hacking activities and associated increased regulatory scrutiny regarding the valuable health data people are providing the world. There may also be discussion of the social responsibilities and plaintiffs’ lawyers may argue to impose a new “duty to warn” for companies that can track your search results or biometric history to catch health conditions you may not yet be aware of.
7. The Possibility of U.S. Federal Data Breach Legislation

In 2017, criminals have hit significant troves of data; state actors have damaged major corporations; and companies have learned that a poorly conceived breach response can do more damage to them than the breach itself.

In the wake of all this, there has been renewed talk in Washington of possible U.S. federal data breach legislation. The current patchwork of sometimes significantly different state laws across the country could provide a possible target for bipartisan policymaking. However, there is always controversy any time federal preemption of state standards is involved. In any event, betting against federal data breach legislation has been the right call every year since California adopted the first state notification law in 2003.

8. A Pivot Toward Asia for Privacy and Cybersecurity Laws

After years of EU-U.S. dialogue on privacy and cybersecurity, we expect an increasing focus on Asia in 2018. China’s major cybersecurity legislation went into effect 2017, but experts are still unclear on its precise contours and requirements. China’s recent steps follow other countries in imposing new regulatory standards that will authorize intrusive government compliance reviews. For example, the Chinese law requires network operators to store select data within China and allows the government to conduct spot-checks on a company’s network operations. More recently, the Indian Supreme Court held that privacy is a fundamental right, prompting an intense effort to develop data privacy legislation in India. And Singapore is considering introducing major cybersecurity legislation in 2018. Malaysia and Indonesia have also taken steps to increase required cybersecurity protections. Japan is expected to complete discussions to establish adequacy under the EU regime in 2018, followed in quick succession by South Korea.

Watch Asia in 2018 for new privacy and cybersecurity requirements that will impact how businesses can operate in the region. A number of countries are suggesting data localization as a way to secure their systems, which would mean significant changes for companies operating there.

9. SEC on Cybersecurity and Rise of Shareholder Breach Litigation

New cybersecurity regulators are appearing every day, it would seem: for example, the last day of 2017 marked the deadline for defense contractors having to comply with the Department of Defense’s new cybersecurity requirements, and there’s the possibility that similar requirements could be coming down the pike for civilian contractors. But of all these potential regulators, the SEC may be able to claim a special role given its duty to protect the integrity of the U.S. financial markets. Indeed, the growing number and complexity of cybersecurity risks has motivated the SEC to play a bigger role in cybersecurity efforts in recent years. Armed with a cyber unit formed in September 2017, new leadership for its Office of Compliance Inspections and Examinations (OCIE), and a clear mandate to focus on cybersecurity governance obligations of public companies, the SEC may be a more significant player by 2019. Although the SEC has yet to sanction a public company for failure to disclose a data breach, it has investigated companies for their handling and reporting of incidents and risks. Given the increased SEC focus, as well as the threat of shareholder actions, public companies should continually review the adequacy of their disclosures relating to cybersecurity risks and cyber incidents.
10. State Cybersecurity and Data Breach Laws

In light of the federal government’s restrained approach on cybersecurity and data breach legislation, the states have increased their policymaking in recent years. State legislatures, insurance commissions, attorneys general and regulatory agencies are moving to develop detailed cybersecurity requirements. In 2017, the New York Department of Financial Services finalized some of the most stringent, and certainly some of the more complex, cybersecurity rules in the country. We expect that such activity will only increase in 2018 as states attempt to take action to fill a perceived federal void. Moreover, taking action against cybersecurity threats appears to be politically enticing – at least at the state level, with the National Conference of State Legislatures counting at least 240 bills on the subject in 42 states. Unfortunately, however, this trend means that companies will be subject to an even more complex patchwork of state laws that impose different and potentially conflicting standards and requirements, increasing the regulatory compliance burdens with limited added benefits.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

Colleen Brown  
Partner  
cfbrown@sidley.com  
+1 202 736 8465

Christopher Fonzone  
Partner  
cfonzone@sidley.com  
+1 202 736 8445

William RM Long  
Partner  
wlong@sidley.com  
+44 20 7360 2061

Geeta Malhotra  
Partner  
gmalhotra@sidley.com  
+1 312 853 7683

Edward McNicholas  
Partner  
emcnicholas@sidley.com  
+1 202 736 8010

Wim Nauwelaerts  
Partner  
wnauwelaerts@sidley.com  
+32 2 504 6210

Alan Charles Raul  
Partner  
araul@sidley.com  
+1 202 736 8477

Yuet Ming Tham  
Partner  
yuetming.tham@sidley.com  
+852 2509 7645

Cameron F. Kerry  
Senior Counsel  
ckerry@sidley.com  
+1 617 223 0305

Sidley Privacy, Data Security & Information Law Practice

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyberlaw. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property and white collar lawyers. We frequently advise regarding HIPAA and Healthcare Privacy issues.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.