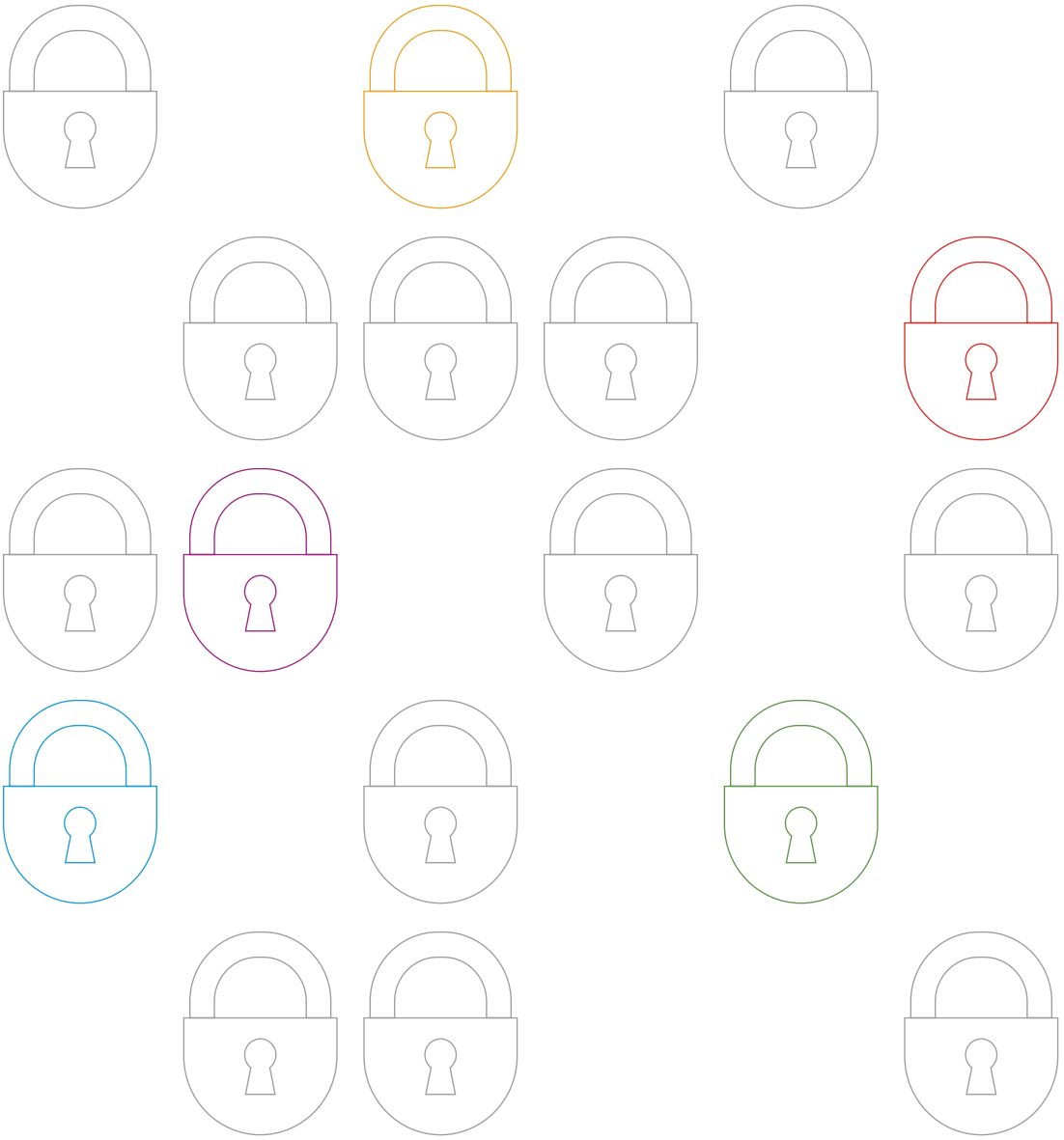
WINSTON & STRAWN LLP

2016 Privacy Year In Review



Privacy and data security issues continued to be a major focus for companies in 2016. Winston & Strawn has once again compiled its *Privacy Year in Review* to help make sense of the many changes that happened this year.

As you plan for 2017—whether in your role as chief legal officer, chief technology officer, chief privacy officer, or anyone who worries about privacy for your organization—**this summary will give you a roadmap of possible issues your company will face in the new year.**

Winston Privacy Institute

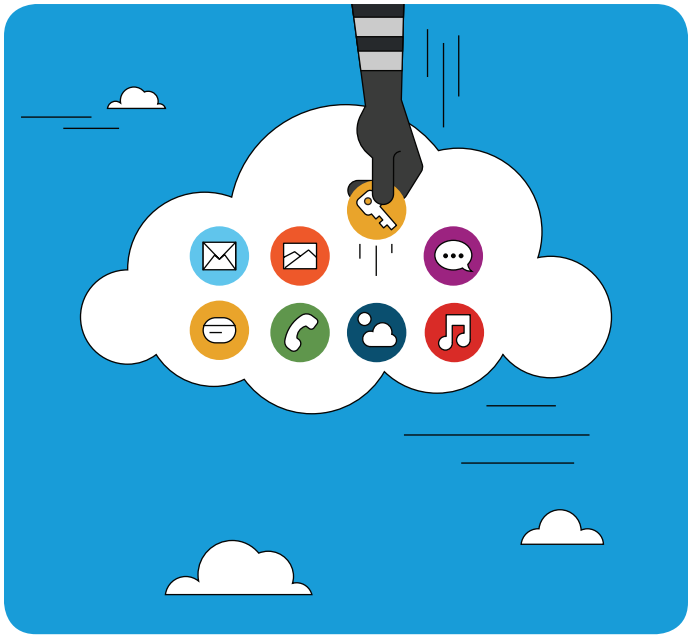
The Winston Privacy Institute brings together events, training, and education on cutting-edge privacy issues.

Summary of Contents

1 Harm-Based Data Breach Suits Continue

Companies that suffer data breaches continue to be concerned that after providing notice, they will face class action lawsuits. A common defense has been to argue that the plaintiffs have not suffered harm. In the spring of 2016, the Supreme Court ruled in *Spokeo, Inc. v. Robins* that statutory violations alone were not enough to satisfy the injury requirement for standing because such alleged harms were not concrete; however, the justices added the caveat that a concrete harm need not necessarily be tangible. What is "harm" is thus unclear. Going into 2017, there remains confusion as to whether or not a data breach-related lawsuit will be dismissed because there has been no harm.

This confusion played out in the courts in the second half of 2016, and will likely continue. For example, a federal district judge in New Jersey ruled in October that a class of plaintiffs lacked standing to sue J. Crew for allegedly including too many credit card digits on customer receipts. In that case, *Kamal v. J. Crew Grp., Inc.*, plaintiffs argued that they



were harmed because the extra credit card numbers on the receipts would expose them to potential future identity theft. The judge ruled that the mere heightened risk of future identity theft is not a concrete harm. However, in two unrelated cases in Florida involving the same credit card receipt issue, the courts found that an increased risk of future identity theft was concrete enough to establish standing. We expect to see more divided cases in the coming year.

Going into 2017, there remains confusion as to whether or not a data breach-related lawsuit will be dismissed because there has been no harm.

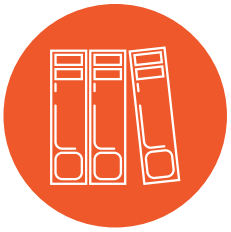
2 Time to Prepare for New European-Wide Privacy Regulation

As a result of the passage in 2016 of the EU General Data Protection Regulations (GDPR), multinational companies will spend much of 2017 preparing for compliance. The regulation goes into effect in May 2018, and will impose significant penalties for non-compliance. It differs from the current privacy regime in Europe, under which Member States have implemented their own national legislation to effectuate the EU Data Protection Directive (Directive 95/46/EC). Instead, the GDPR regulation has Europe-wide effect without the need for national legislation.

Several critical differences distinguish the GDPR from the Directive. These differences will require many companies to assess their current practices and create new internal procedures to ensure compliance. For example, the GDPR includes a "right to be forgotten." Under this right, individuals can ask the data controller to delete their personal information. Companies will also have to keep detailed records of their data-processing activities. This replaces prior DPA registration requirements that exist in some jurisdictions.

Certain companies will also be required to have a data protection officer. In addition, there are provisions for how to handle data breaches and the types of security required for personal information. As we move into 2017, we expect to see multinationals spending time and energy understanding the new law's requirements.

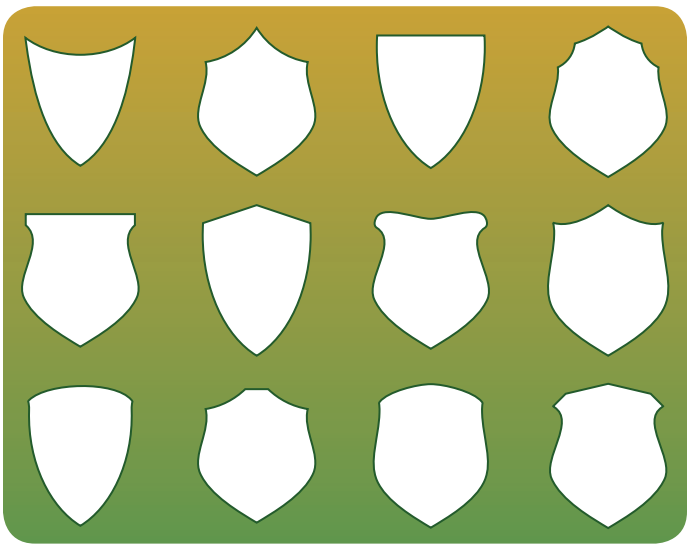
The regulation goes into effect in May 2018, and will impose significant penalties for non-compliance.



3 Privacy Shield May Gain More Traction—Or Not...

The EU-U.S. Privacy Shield—successor to Safe Harbor—went live in August 2016. The program gives European companies wishing to export data to companies in the United States an avenue to do so without violating EU privacy laws. There are other options, including executing model clauses. Indeed, after Safe Harbor was called into question in October 2015, many companies executed model clauses.

Now, doubts around the Shield are causing several organizations—including those that previously participated in Safe Harbor—to consider giving Privacy Shield a miss. Chief among the concerns is that the EU Commission will re-evaluate the effectiveness of the Shield each year. Presumably, if the Commission has concerns, it will decide that EU companies can no longer rely on the Shield as a basis for the transfer of information. Other prime concerns have centered around the level of contractual provisions that need to be in place with third parties with whom the U.S. entity shares EU information, and the Department of Commerce's assertions that it will be giving participants greater scrutiny than it did under Safe Harbor.



However, privacy officers and lawyers within organizations have seen the Shield as an opportunity to bring focus to their companies' privacy activities. Why? Because part of the process for a U.S. company considering the Shield is to assess current practices and determine that it can live up to the promises it needs to make. Thus, a company might go through the process of getting ready for the Shield—falling short of actually signing up for the program—and use the preparation exercise for ensuring general privacy compliance or, for a multinational, preparing for GDPR.

4 Increasing Need to Protect "Internet of Things"

Everyone has begun to think more about the Internet of Things—and protecting connected devices—following a massive hack of connected devices in October 2016. Of particular concern for the FTC, and others, has been whether companies are using reasonable security measures to ward off a hacking attack. The October incident, for example, targeted connected devices that had default usernames and passwords.

We expect to see greater scrutiny by the Federal Trade Commission and others around connected devices, and the security measures companies use to protect those devices and the information that resides on them. This would follow a trend we started to see in 2016. For example, in February, the FTC settled with ASUSTeK, a cloud computing and router company, over alleged gaps in ASUSTeK's products' security—gaps that the FTC said constituted a violation of its

We expect to see greater scrutiny by the Federal Trade Commission and others around connected devices

promises of protecting consumers. Similarly, at the end of 2016, 15 state attorneys general settled with Adobe for $1 million after a data breach impacting more than half a million users. Of concern for the AGs was Adobe's alleged lack of mechanisms to detect and respond to unauthorized activity in its systems.

Offering some help for companies designing interconnected devices may be recent NIST guidance that purports to assist businesses build security into products' life cycles. The publication ("System Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems") was released in November 2016.

5 Privacy and Security Changes Coming in China

In November, the Chinese government passed a comprehensive cybersecurity law that is causing concern for non-Chinese organizations. In particular, the law permits the Chinese government to audit organizations and potentially release source code and encryption keys to the government. For certain industries, the law also requires governmental permission before transferring personal information out of the country. This new cybersecurity law is set to go into effect in June 2017. As a result, companies with Chinese operations are assessing their security and data transfer policies.

Further, in the summer of 2016, the State Administration of Industry and Commerce solicited comments on proposed regulations to implement the existing Consumer Rights Protection Law. Under the regulation, the amount of personal information that can be collected would be limited to that which is relevant to the company's business operations. Where consumer consent is required, records of that consent would need to be kept for five years. These developments suggest that additional privacy legislation may be coming in 2017.

Companies with Chinese operations are assessing their security and data transfer policies.

For certain industries, the law also requires governmental permission before transferring personal information out of the country.

6 Industry-Specific Privacy Requirements Continue to Proliferate

It seems like every federal regulator wants to get in on the privacy action these days. We are watching to see if this trend continues in 2017. The requirements being imposed on organizations by this ever-increasing alphabet soup of regulators is not always consistent.

For example, in October, the Federal Communications Commission's privacy regulations for broadband providers was passed. Compliance deadlines are coming up in 2017 and 2018. Several state attorneys general have expressed concern about the regulations, which will require covered entities to get express prior consent (i.e., opt-in consent) from customers before collecting "sensitive" data. Sensitive data is broadly defined, however, and includes children's information, health and financial information, geolocation records, and internet browsing history. This opt-in regime conflicts with the FTC's opt-out approach. The AGs' fear is that not only might this law preempt state privacy laws, it adds yet another layer to an already complex patchwork of privacy laws. While the regulation may be challenged, it is not likely to be the last such legislation coming from Washington, D.C.

In the financial services arena, the Consumer Financial Protection Bureau began its enforcement efforts in 2016. In its first-ever case, the agency now charged with enforcing federal consumer financial laws settled with the digital payment platform Dwolla over alleged inadequate data security measures. The CFPB asserted that Dwolla failed to encrypt sensitive data, did not conduct risk assessments, and did not train employees on data security. Dwolla agreed to pay $100,000 and take corrective steps to improve its data security.

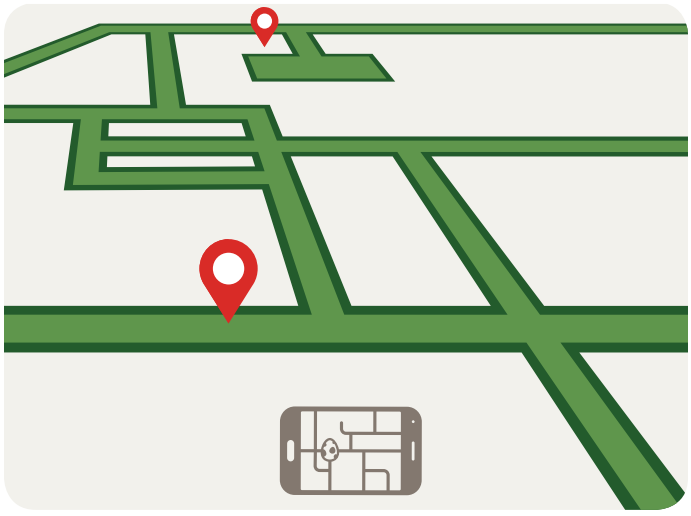
As requirements on organizations proliferate, having a clear understanding of what information a company holds, how it gets it, how it is used, how it is protected, and what the most common security vulnerabilities are will be invaluable in 2017.

7 Consumers Aren't Letting Go of Their Phones Anytime Soon

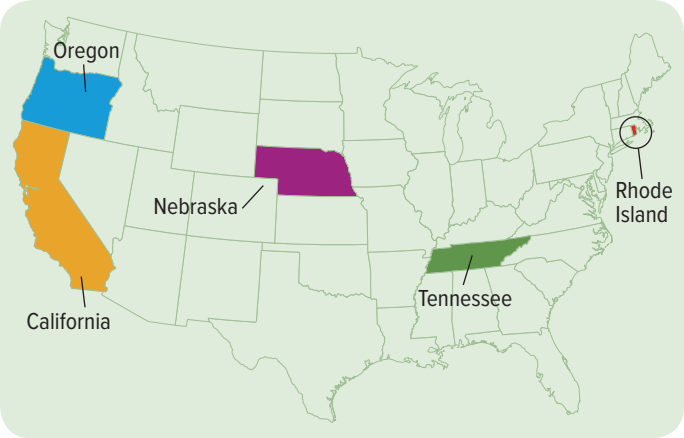
Pokémon GO brought augmented reality—and related privacy concerns—to the forefront in 2016. As consumers hunted for Pokémon characters in their neighborhoods and beyond, regulators worried about the geo-location data collected by the creator, Niantic, Inc. The FTC received dozens of consumer complaints about the app's tracking, and the company was questioned by Congress. More companies will likely join the augmented reality arena in 2017, and as they do, they would be well served to keep in mind regulators' concerns.

Providing assistance is the Digital Advertising Alliance's mobile privacy guidelines. That document provides guidance around how to give consumers clear and conspicuous information about the collection of precise location data. In a settlement with mobile health app iTriage LLC, iTriage and the Accountability Program (which enforces the DAA guidelines) agreed that the company would cease collecting and providing precise geo-location data to third parties. The FTC has also focused on the issue, and in June 2016 settled with InMobi, a mobile advertising network, for allegedly bypassing location settings on users' phones to collect precise location data. As part of the settlement, the company agreed to pay almost $1 million and to stop collecting location information without users' express consent. The company also agreed to delete information already collected and to conduct privacy audits every two years for the next two decades.

Companies might use location data to interact with consumers through mobile apps, but many consumers continue to use mobile phones for two basic functions: sending texts and making calls. Under federal regulations (the Telephone Consumer Protection Act), autodialed calls or texts to cell phones cannot be made without consent, and if the content of the message is advertising in nature, specific language must be in the consent request. Further, the consent itself must be signed (a digital signature will suffice). Consumers are most easily reached on their cell phones. This, coupled with the rigorous consent requirements, will result in continued cases involving auto-dialed calls or text messages to cell phones.



8 More Changes to Track in State and European Data Breach Laws



The trend among U.S. states of continually tweaking their data breach notification laws has not changed. In 2016, five states had modifications to their breach notification laws that went into effect (California, Nebraska, Oregon, Rhode Island and Tennessee). California has already made additional changes that will go into effect in 2017. This marks the sixth time that the California law has been modified. Illinois, too, had changes that will go into effect on January 1. Also looming on the horizon is the breach notification requirements in Europe under GDPR that will go into effect in May 2018.

Some U.S. states expanded the definition of triggering personal information. However, save for modifications to add health-related (or biometric) information, these changes merely reflected provisions that existed under other states' laws. Several states—California, Illinois, Nebraska and Tennessee—tweaked how they handle encrypted information. Other modifications included timing of notice to individuals and the addition of a requirement to notify the relevant attorneys general.

From a timing perspective, of greatest concern may be the 72-hour window companies will have in Europe to notify their supervisory authorities after discovery of a breach. The 72-hour time must be met "if feasible." If there is a delay—and such reasons for a delay have not yet been explored by the EU—the company must explain the reason for the delay. It remains to be seen what would constitute a reasonable delay; for example, would working with law enforcement be reasonable, as is the case in the United States? Or investigating to understand the scope of the incident? Also unclear is when the clock will begin to tick (i.e., when is a "breach" discovered?).

We expect to see continued tweaks to breach notice statutes, as well as additional countries enacting notice requirements in 2017. For example, Australia currently has a breach notification bill pending, which some expect might be passed and go into effect by the end of 2017.

Winston Privacy Institute