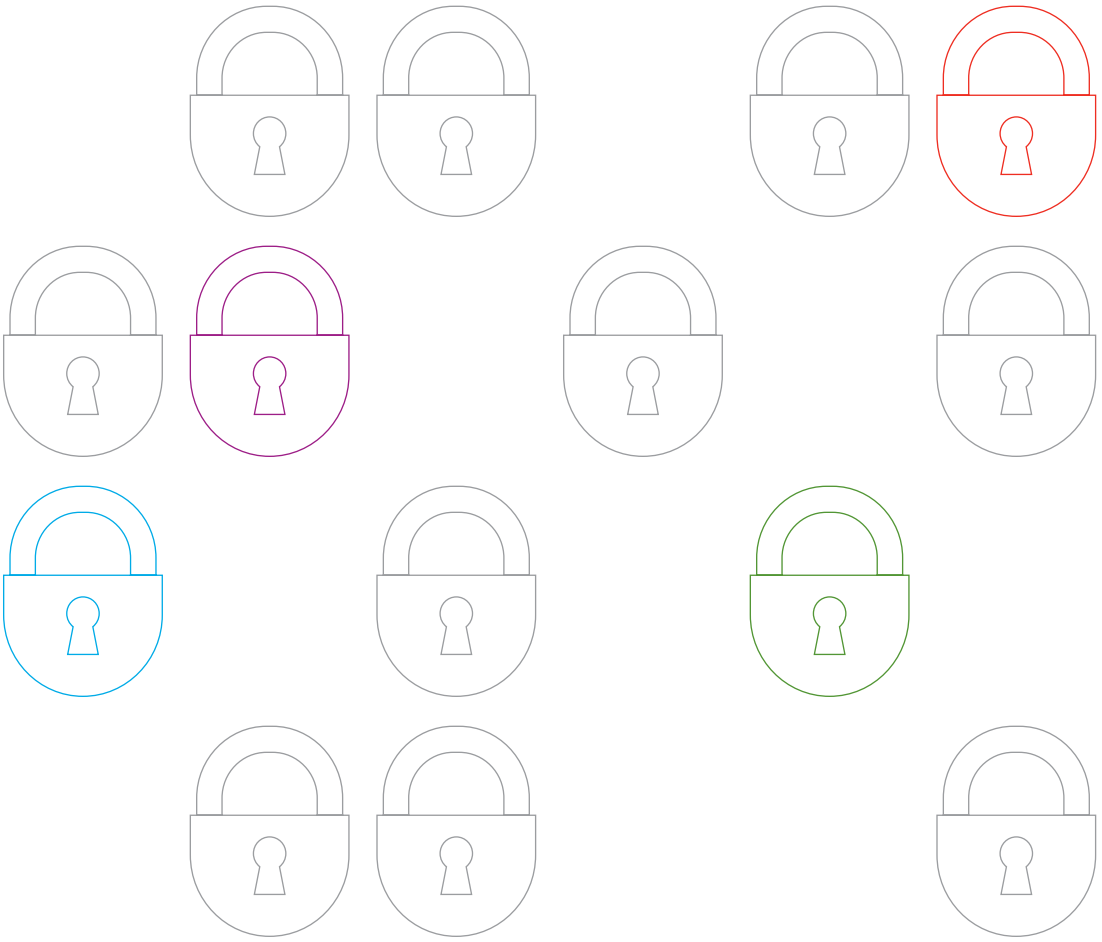
WINSTON & STRAWN LLP

2018 Privacy Year in Review

Navigating Compliance in a Shifting Privacy Landscape



1 GDPR Enforcement in 2018

On May 25, 2018, the EU General Data Protection Regulation ("GDPR") finally became enforceable. Although data breach reports have more than quadrupled since, enforcement actions have rolled out with significantly less fanfare. On July 11, the UK's Information Commissioner's Office ("ICO") quietly filed the first GDPR enforcement order, buried within the annex to a report on investigations into political groups. But while Facebook and Ticketmaster have become the face of what not to do in the post-GDPR world, neither company has been cited for GDPR violations. The ICO fined Facebook €500,000 in October for "lack of transparency and security issues," but the fine was pursuant to the Data Protection Act of 1998, the applicable law at the time of Facebook's conduct. Meanwhile, while many expected Ticketmaster's delay in reporting a data breach to be the litmus test for GDPR enforcement, the ICO is still deliberating whether to issue a fine.

Instead, Canadian data analytics firm AggregateIQ Data Services Ltd. ("AIQ") was the first recipient of an enforcement action. The ICO alleged that AIQ received personal data of UK citizens from political organizations and used this data to target those people with political advertising without their knowledge or consent.

Enforcement actions have since accumulated. In late July, France's Data Protection Authority published a warning to two French companies for failing to obtain valid consent for the use of location data for profiling and targeted advertising. In November, Germany's Data Protection Authority ("LfDI") fined a chat application provider €20,000 after hackers stole unencrypted data concerning approximately 330,000 consumers. A few weeks later, several EU countries filed complaints against Google, alleging that the company is tracking Android users' location history without prior consent.

As GDPR complaints grow to include some of Silicon Valley's largest companies, the law's impact on the United States remains to be seen. The ICO and the LfDI have stressed that the emphasis in these actions is on education and improved data security for users, rather than punitive fines. Indeed, the first wave of GDPR remediation has largely involved organizations adding check boxes to their websites and other forms of communications with customers. However, with the increase in state-specific privacy laws and the looming possibility of federal privacy legislation, GDPR compliance may soon be the least of a company's worries.

2 Enactment of California's Consumer Privacy Act

In late June, Governor Jerry Brown signed the California Consumer Privacy Act ("CCPA"), making California the first state to pass a GDPR-inspired state privacy law. However, the law does not go into effect until 2020, giving the California Attorney General the necessary time to promulgate the regulations that will guide compliance. Generally speaking, the CCPA sets specific parameters on how businesses collect, store, and use consumers' personal data. Although the CCPA protects California residents, businesses around the world must comply with the law, if they receive personal data from California residents and exceed one of three thresholds: (a) annual gross revenues of $25 million; (b) obtaining personal information ("PI") of 50,000 or more California residents, households or devices annually; or (c) 50 percent or more annual revenue from selling California residents' PI.

The law can best be described by a simple word—control. Specifically, the law gives consumers more control over their PI. Indeed, the CCPA purports to accomplish three goals: (1) giving consumers the right to know what information large corporations are collecting about them; (2) giving consumers the right to tell a business not to share or sell their PI; and (3) giving consumers the right to protections against businesses that compromise their PI. The law grants consumers all of these rights and more, including the right to request deletion of their PI.

Although these goals appear consistent with the GDPR, businesses cannot assume that their GDPR-compliant measures will be sufficient to achieve compliance with the CCPA. For example, the CCPA contains a broader definition of what constitutes "personal data," and the laws use different standards to govern the level of consumer consent required to collect consumer data. Businesses are, therefore, encouraged to assess the CCPA's impact on their business, systems, and data handling practices.

This CCPA changes the landscape of data privacy in the United States, and the new law is likely just the beginning. Following the CCPA, several states, including Vermont and Ohio, passed legislation tackling other privacy and cybersecurity issues. Additionally, Washington continues to hear a growing crescendo demanding this type of legislation. On the federal side, Congress introduced two privacy bills at the end of last year. In 2019, the issue will surely continue to grow and spur federal debate.

3 California's Cybersecurity Law Requiring Reasonable Security Measures

This year, California also passed Senate Bill 327 ("SB 327"), widely recognized as California's and the nation's first Internet of Things ("IoT") Cybersecurity Law. Like the CCPA, SB 327 will not go into effect until January 1, 2020, allowing time for the promulgation of guidance regulations. When it does take effect, SB 327 will require manufacturers of Internet-connected devices that are sold or offered for sale in California to equip the devices with "reasonable security features" designed to protect against unauthorized access, destruction, use, modification, or disclosure.

The bill only applies to "manufacturers" and defines a "connected device" as any device or other physical object that is capable of connecting to the Internet directly or indirectly and that is assigned an IP or Bluetooth address. Although SB 327 is intentionally vague as to what constitutes a "reasonable security feature," it provides some broad parameters and examples of specific approaches that may satisfy the requirement. In lieu of a strict definition, lawmakers and regulators have compiled guidance documents—such as guidelines from the Federal Trade Commission ("FTC") and National Institute of Standards and Technology ("NIST")—that outline best practices and security features that may qualify as "reasonable."

Although SB 327 will only apply to devices sold or offered for sale in California, national manufacturers should avoid creating California-specific designs and instead opt for uniform changes across production. As momentum builds to pass an analogous federal privacy bill, SB 327's requirements may become nationwide requirements within the span of a few years.

"When it does take effect, **SB 327 will require manufacturers of Internet-connected devices that are sold or offered for sale in California to equip the devices with 'reasonable security features'** designed to protect against unauthorized access..."

4 Significant Developments in Data Breach Notification Legislation

In 2018, data breach notification laws passed in South Dakota and Alabama, which means that now all 50 states and the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation governing data breach notification requirements.

Additionally, Colorado and Louisiana passed significant amendments to their existing data breach notification laws in 2018, while Vermont passed the first privacy law directed specifically to data brokers, which includes, among other things, annual reporting and disclosure requirements.

- *Colorado*. Among other things, Colorado's amendment expanded the definition of personal information and existing data security breach notification obligations. Under the amendment, personal identifiable information also includes an individual's name in combination with a student, military, or passport number, medical information, a health insurance identification number, biometric data, or online access credentials. Colorado also now enforces stricter notification requirements for both affected individuals and the state Attorney General. Additionally, notice letters must now include more detailed information, including a statement that the resident may obtain further information from the FTC and consumer reporting agencies regarding fraud alerts and security freezes. If the acquired data included online access information, the notice must also include a statement to change the password or otherwise take steps to protect affected accounts.

- *Louisiana*. Louisiana amended its data breach notification law to require entities to notify affected residents of a breach within 60 days of the discovery of a breach. If the notice is delayed for certain purposes including, for instance, to determine the scope of the breach, to prevent further disclosure, or to cooperate with a law enforcement investigation, entities must notify the state Attorney General within the 60-day period, who will then grant an extension after receiving a written explanation for the reasons for the delay. The amendment also expanded the definition of personal identifiable information to include the person's name together with a passport number or biometric data.
- *Vermont*. The first of its kind, as of January 1, 2019, Vermont imposes notification obligations on "data brokers," which are defined as entities that "knowingly collect[] and sell[] or license[] to third parties the brokered personal information of a consumer with whom the business does

not have a direct relationship." Under the law, data brokers must disclose to the state Attorney General information about how they collect, store, or sell consumers' personal information, including any practices allowing opt-outs. The law also requires data brokers to report security breaches on an annual basis. A violation of this data broker law amounts to an unfair and deceptive act in violation of Vermont's consumer protection law.

- *Canada*. Significantly, Canada's privacy breach reporting requirements also came into effect in 2018. All entities subject to Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") must notify individuals of any breach of the security of safeguards involving their personal information if it is reasonable to believe that the breach creates a "real risk of significant harm." Organizations must also report a breach to the Privacy Commissioner of Canada. Additionally, notification to private third parties may also be required if such parties are believed to be able to mitigate or reduce the risk of harm to affected individuals. While the law does not specify a certain timeframe within which to give notice, such notice must be "as soon as feasible" after the organization determines the breach has occurred. The new regulation also requires that organizations maintain certain records of every breach for 24 months after any such incident, which the Privacy Commissioner may request at any time.

5 Biometric Legislation & Litigation

The wave of class action litigation under Illinois' Biometric Information Privacy Act ("BIPA") continued unabated in 2018, with scores of complaints filed at both the state and federal level. BIPA is one of three state laws (the other states being Texas and Washington) that specifically regulates the collection, storage, and dissemination of biometric data. However, BIPA is unique in that it allows for a private right of action as well as statutory penalties. Under these laws, before collecting an individual's personal information, an organization must obtain the individual's consent (which must be written under BIPA), inform the individual of its privacy and data retention practices, and be reasonable in protecting the collected data.

In 2018, the battle lines in BIPA litigation were drawn on determining what amount of harm is necessary to establish a claim. This argument took two related paths. At the federal level, defendants have argued with moderate success that mere technical violations of the law (e.g., failing to obtain written consent) without some type of actual harm (e.g., a data breach resulting in identity theft) is insufficient to establish Article III standing under the *Spokeo* standard. Similarly, in order to establish a claim under the statute, a person must be "aggrieved," which defendants have interpreted to require actual harm beyond a technical violation. Two Illinois state appellate courts have reached opposite conclusions on whether technical violations are a sufficiently cognizable injury to a person's privacy to aggrieve someone under the law; an appeal is currently before the Illinois Supreme Court that will provide some clarity on how broadly to define "aggrieved" under the law.

6 Regulation of Emerging Technology: Developments in AI/ALPR Legislation

"As privacy laws struggle to catch up to new technologies, several states passed new laws this year to regulate previously ungoverned technologies."

As privacy laws struggle to catch up to new technologies, several states passed new laws this year to regulate previously ungoverned technologies. One such prominent example is the increasing number of laws governing the collection and use of automatic license plate readers ("ALPR"). ALPR systems are a new type of artificial intelligence technology ("AI") either fixed or attached to mobile vehicles and are constantly capturing and storing individuals' license plates. These pictures are stored in massive databases and are used to create geographic mosaics of a car's (not necessarily an individual's) location over time. These systems are primarily used by law enforcement agencies, but are also used by insurance and financial lending companies. In 2018, several states introduced or passed laws regulating how law enforcement agencies may collect such data and for how long the data may be stored. Only a small number of states currently regulate the commercial use of ALPR systems, but several laws are currently pending.

7 FCC Clashes with Courts Over TCPA Interpretation and Enforcement

The Telephone Consumer Protection Act ("TCPA") prohibits the use of certain automated dialing equipment to call wireless telephone numbers without consent. One of the practices regulated by the TCPA is the use of "automatic telephone dialing systems" ("ATDS"). An ATDS is defined as equipment with the "capacity" to dial numbers that were stored or produced using a random or sequential number generator. Under a 2015 FCC declaratory order, "capacity" was defined broadly to include a device's current configuration and its "potential functionalities."

Last December, however, in *ACA International v. FCC*, the U.S. Circuit Court of Appeals for the District of Columbia vacated the FCC's broad definition of "capacity." The D.C. Circuit observed that the sweeping interpretation would include all smartphones, given that all such devices can be customized to produce, store, and call random numbers, thereby rendering nearly every American into a "TCPA-violator-in-waiting, if not a violator-in-fact." The Third Circuit also adopted the D.C. Circuit's reasoning and rejection of the FCC interpretation. However, in *Marks v. Crunch San Diego, LLC*, the Ninth Circuit moved in the opposite direction, expanding the definition of "capacity" beyond even the FCC's interpretation. In response to this circuit split, the FCC has sought comment on the definition of ATDS.

The TCPA also regulates instances when an autodialer contacts a number, for which the autodialer previously had consent to contact, but which has subsequently been reassigned to an individual, who has not provided consent. The FCC ruled that contacting these "reassigned" numbers constituted a violation, but that the caller would be afforded a one-call, post-reassignment safe harbor. Then in December 2018, after the D.C. Circuit vacated the FCC's ruling, the FCC responded by creating a national database of reassigned numbers.

In 2019, the Supreme Court may resolve these clashes between the FCC and Federal Circuit courts by issuing a ruling in *PDR Network LLC v. Carlton & Harris Chiropractic Inc.* that clarifies whether courts may independently interpret the TCPA or must defer to the FCC. We may also see the passage of the bi-partisan TRACED Act, which would broaden the authority of the FCC and other agencies like the Consumer Financial Protection Bureau ("CFPB") to enforce the TCPA.

8 The SEC Brings its First Enforcement Action Under the Identity Theft Red Flags Rule

In late September, the Securities and Exchange Commission ("SEC") brought and settled the first enforcement action brought under the Identity Theft Red Flags Rule ("Red Flags Rule") since its adoption in 2013. Among other charges, the SEC charged broker-dealer and investment adviser Voya Financial Advisors Inc. ("VFA") with violating the Red Flags Rule's requirement that financial institutions implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations.

According to the SEC's order, VFA maintains a web portal for independent contractors to access customer information and process transactions. Cyber intruders impersonated VFA contractors over a six-day period in April 2016 by calling VFA's support line and requesting that the contractors' passwords be reset. In two of these instances, the intruders used phone numbers that VFA had previously identified as associated with fraudulent activity premised on the same conduct. Nevertheless, VFA's technical support provided temporary passwords over the phone, thereby granting the intruders access to the personal information of over 5,000 VFA customers.

The SEC found that although VFA adopted an Identity Theft Program in 2009, it violated the Red Flags Rule because it did not review and update the program in response to the changes in risks to its customers, nor did it provide adequate training to its employees. Additionally, the program did not include reasonable policies and procedures to respond to identity theft red flags, such as those detected by VFA during the April 2016 intrusion. Without admitting or denying the SEC's findings, VFA agreed to be censured and pay a $1 million penalty.

This action highlights the importance of conducting regular reviews of incident response protocols and ensuring proper training. With the proper training in place, VFA could have avoided this unfortunate incident.

"The SEC found that although VFA adopted an Identity Theft Program in 2009, it violated the Red Flags Rule because it did not review and update the program..."

9 The Supreme Court Expands Digital Privacy Rights in *Carpenter v. United States*

This summer, the Supreme Court again applied centuries-old language to the technological realities of the present. In *Carpenter v. United States*, the Court held that the government needs a warrant to access cell site location information ("CSIL"), which is automatically generated whenever a cell phone connects to a cell tower and is stored by wireless carriers for years. Cell phone location records are therefore subject to Fourth Amendment protections.

In *Carpenter*, prosecutors sought to corroborate testimony that Timothy Carpenter participated in a series of armed robberies in the Detroit area. The FBI obtained Carpenter's CSIL from wireless carriers under the Stored Communications Act ("SCA"), which requires the government to provide facts showing there are "reasonable grounds" to believe that data being sought is relevant to an ongoing investigation. This standard does not require a warrant and is lower than the Fourth Amendment's standard, which requires a warrant where an individual demonstrates a legitimate expectation of privacy. The records showed that Carpenter's phone had been within a two-mile radius of the robberies when they took place, corroborating witness testimonies that Carpenter was involved.

In holding that the government's acquisition of Carpenter's CSIL constituted a search, the Court determined that the "third-party doctrine," which provides that information you voluntarily share with a third party is not protected by the Fourth Amendment, could not be applied to cell phone technology. This decision was a departure from decades of jurisprudence. Indeed, the Court has previously relied on the "third-party doctrine" to hold that the government does not need a warrant to access a defendant's banking records or call records. The Court suggested, however, that the third-party doctrine is questionable in today's world. A cell phone is "almost a feature of human anatomy," and tracking a cell phone can therefore achieve "near perfect surveillance" akin to GPS monitoring. This, according to the Court, violates a person's reasonable expectation of privacy.

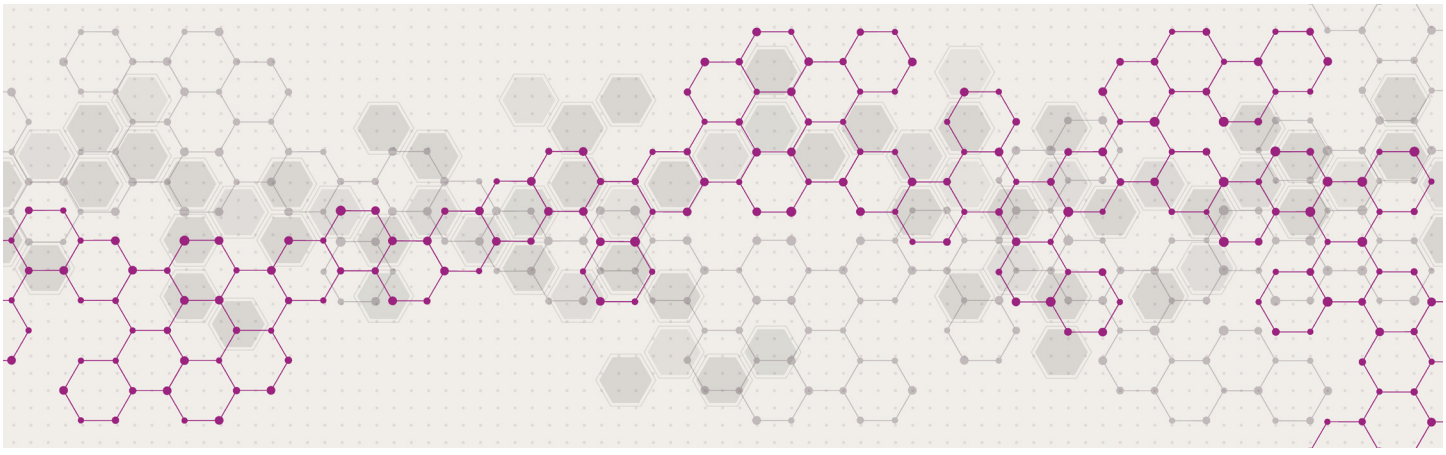
Carpenter is the most recent Supreme Court case to expand data privacy protections. In the 2012 case *United States v. Jones*, the Court ruled that police need a warrant to place a GPS tracker on a car. In the 2014 case *Riley v. California*, the Court ruled that police need a warrant to search an arrestee's cell phone. With data privacy litigation on the rise, it begs the question of whether the time has come to update the Fourth Amendment for the digital age.

10 Anthem's $16 million HIPAA Settlement

On October 18, 2018, Anthem, Inc. ("Anthem"), one of the nation's leading health benefits companies, agreed to pay $16 million to the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") to settle its potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Anthem also agreed to undertake a robust corrective action plan to comply with the HIPAA rules. Separately, on August 15, 2018, the court also granted final approval of a settlement of $115 million to resolve the multidistrict class action litigation relating to the cyber-attack precipitating Anthem's potential HIPAA violations.

According to OCR's investigation and Anthem's report, at some point between December 2, 2014, and January 27, 2015, cyber-attackers gained access to Anthem's IT system through spear phishing emails sent to an Anthem subsidiary. The attackers stole the electronic protected health information ("ePHI") of almost 79 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information. OCR also discovered additional potential violations of the HIPAA rules, including: (A) a failure to conduct accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI held by Anthem, (B) a failure to implement sufficient procedures to regularly review records of information system activity, (C) a failure to identify and respond to detections of the security incidents leading to this breach, and (D) a failure to implement sufficient technical policies and procedures to control access to ePHI.

This action is the largest health data breach and the largest HIPAA enforcement to date. As OCR Director Roger Severino commented, "large health care entities are attractive targets for hackers, which is why they are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion or risk enforcement by OCR."



Editors

Sheryl Falk
Partner, Houston
+1 (713) 651-2615
sfalk@winston.com

Alessandra Swanson
Of Counsel, Chicago
+1 (312) 558-7435
aswanson@winston.com

Shawn Obi
Associate, Los Angeles
+1 (213) 615-1763
sobi@winston.com

Eric Shinabarger
Associate, Chicago
+1 (312) 558-8823
eshinabarger@winston.com

About Winston & Strawn

Winston & Strawn LLP is an international law firm with 1,000 attorneys across 16 offices in Brussels, Charlotte, Chicago, Dallas, Dubai, Hong Kong, Houston, London, Los Angeles, Moscow, New York, Paris, San Francisco, Shanghai, Silicon Valley, and Washington, D.C. The exceptional depth and geographic reach of our resources enable Winston & Strawn to manage virtually every type of business-related legal issue. We serve the needs of enterprises of all types and sizes, in both the private and the public sector. We understand that clients are looking for value beyond just legal talent. With this in mind, we work hard to understand the level of involvement our clients want from us. We take time to learn about our clients' organizations and their business objectives. And, we place significant emphasis on technology and teamwork in an effort to respond quickly and effectively to our clients' needs.

Visit **winston.com** if you would like more information about our legal services, our experience, or the industries we serve.