GIBSON DUNN

January 28, 2019

U.S. CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2019

To Our Clients and Friends:

In honor of Data Privacy Day—an international effort to raise awareness and promote privacy and data protection best practices—we offer this seventh edition of Gibson Dunn's United States Cybersecurity and Data Privacy Outlook and Review.

In recent years, companies have been challenged to navigate a rapidly evolving set of cybersecurity and privacy challenges. If anything, the pace of this evolution increased in 2018. Federal agencies jockeying for prominence were joined by an increasingly active set of state Attorneys General and other state regulators in enforcing privacy and cybersecurity standards. The California Consumer Privacy Act brought privacy regulation in the United States one step closer to prescriptive European-style controls. With greater frequency, the plaintiffs in privacy class actions survived early attempts to dismiss their claims. Biometric information privacy acts were an active battleground for litigation. And questions regarding the government's ability to access data, whether stored on servers outside the United States or on a cellphone in a target's possession, came into sharp legislative and judicial focus.

This Review places these, and other, 2018 developments in broader context, addressing: (1) the regulation of privacy and data security, including enforcement by federal and state authorities, new regulatory guidance, and key legislative developments; (2) trends in civil litigation, including privacy class actions, interceptions and eavesdropping, biometric information privacy acts, device hacking, and the development of the cybersecurity insurance market; and (3) the collection of electronically stored information by the government, including the extraterritoriality of subpoenas and warrants and the collection of data from electronic devices. While we do not attempt to address every development that occurred in 2018, this Review focuses on a number of the most significant developments affecting companies as they navigate the evolving cybersecurity and privacy landscape.

Our companion International Cybersecurity and Data Privacy Outlook and Review addresses a number of developments of interest to U.S. and international companies alike. These include the entry into force of the European Union's General Data Protection Regulation ("GDPR"), challenges to the EU-U.S. Privacy Shield framework, further developments around the EU Directive on the Security of Network and Information Systems ("NIS Directive") and the EU ePrivacy Regulation, and changes to the privacy and cybersecurity legal landscape in Brazil, Canada, and China, among other countries.

TABLE OF CONTENTS

I. REGULATION OF PRIVACY AND DATA SECURITY

A. ENFORCEMENT AND GUIDANCE

1. Federal Trade Commission

The Federal Trade Commission ("FTC" or "Commission") remained one of the most active and aggressive regulators of privacy and data security in 2018. Operating with new Commissioners and new leadership, the FTC announced eight enforcement actions related to privacy and data security issues as well as a broad-ranging policy review. We address highlights from each of these developments below.

a. Leadership Changes and Policy Review

This year saw an overhaul of the FTC's leadership as President Trump appointed a new Chairman and filled each of the remaining four commissioner seats with new appointees. After a lengthy period during which the Commission was operating at less than full strength, on May 1, 2018, Joseph Simons was sworn in as Chairman of the FTC.[1] Simons previously served in roles at the FTC as Director of the Bureau of Competition, Associate Director for Mergers, and Assistant Director for Evaluation.[2] He was joined by new four Commissioners—Joshua Phillips, Rebecca Kelly Slaughter, and Rohit Chopra, who were confirmed in May,[3] and Christine S. Wilson, who was confirmed in September (to fill departing Commissioner Maureen K. Ohlhausen's seat).[4]

The priorities of the newly constituted Commission remain unclear, but there are strong indications that changes may be forthcoming. As the FTC attempts to balance the current Administration's push for deregulation, growing public pressure for additional privacy enforcement, and the agency's institutional desire for prominence, the form those changes will take is not yet clear. Indeed, the Commission announced this fall that it would undertake a "comprehensive re-examination of the FTC's approach to consumer privacy"—the first such review since 2012—as part of its ongoing "Hearings Initiative," which is a series of policy reviews on a wide range of issues.[5] The FTC's review of data security and

privacy issues has included public hearings and an invitation for comments, and will extend into spring of 2019.

b. Data Security and Privacy Enforcement

Even in the midst of these leadership changes and the policy review, the FTC has continued to announce enforcement actions in this space, in some tension with the purportedly business-friendly administration, although many of these enforcement actions notably included no monetary remedies.

Toy Manufacturer. In January 2018, the FTC pursued its first children's privacy case involving Internet-connected toys.[6] The agency settled with a toy maker in a case alleging that the company violated the Children's Online Privacy Protection Act ("COPPA") by collecting personal information from children without notice or parental consent.[7] The FTC also alleged that the company failed to take reasonable steps to secure the collected data as required under COPPA and that it falsely stated in its privacy policy that personal information obtained through its platforms would be encrypted.[8] As part of the settlement, the company will pay $650,000.[9]

Mobile Phone Manufacturer. The FTC entered into a settlement with a mobile phone manufacturer in April 2018 over allegations that the company allowed collection of consumers' personal information, such as the contents of text messages and location data.[10] The mobile phone manufacturer allegedly collected information without consent and despite promises that the data would be kept secure and private.[11] Specifically, the FTC alleged that the company falsely claimed that only data needed to perform requested services would be collected and that the company had implemented appropriate controls to safeguard consumer information, but in practice failed to do so.[12] The final settlement, which includes no fines or penalties, prohibits the manufacturer from making misrepresentations about its data security and privacy measures, and mandates that the manufacturer establish, implement, and maintain a data security program.[13]

Financial Services Firm. In May 2018, the FTC entered into a settlement with a financial services firm over allegations that the company failed to provide users of its payment service with information about users' ability to transfer funds.[14] The service allegedly told users that money credited to their accounts could be transferred to bank accounts, without disclosing that the funds could be frozen or removed based on the service's review of the underlying transaction.[15] The FTC also alleged that the service's default settings misled consumers about the privacy options for their transactions.[16] The FTC also alleged that the service misrepresented its security systems and violated the Gramm-Leach-Bliley Act's Safeguards and Privacy Rules by failing to maintain adequate security measures and failing to send privacy notices to consumers.[17] The final settlement, which includes no fines or penalties, prohibits the service from misrepresenting any material restrictions on the use of its service, its privacy control settings, and its level of security.[18] The order also requires the service to make disclosures to consumers relating to its transaction and privacy practices.[19] With respect to alleged Gramm-Leach-Bliley Act violations, the service is prohibited from violating the Safeguards and Privacy Rules, and is required to obtain biennial third-party assessments of its compliance for the next 10 years.[20]

EU-U.S. Privacy Shield Enforcement. The FTC brought five actions against companies regarding false claims of certification under the EU-U.S. Privacy Shield framework, which establishes a process to allow companies to transfer consumer data from the European Union to the United States.[21] In July 2018, the FTC settled charges with one company regarding allegations that the company falsely claimed on its website that it was in the process of being certified under the EU-US Privacy Shield framework. In fact, the company had allegedly started an application but had not taken necessary steps to participate in the framework. In September, the FTC announced it had reached a settlement with four additional companies over false claims of certification.[22] Each of the companies claimed to be in compliance with the Privacy Shield, despite allowing their certifications to lapse or never obtaining certification in the first place.[23] Each of the five settlements prohibits the companies from misrepresenting the extent to which they participate in any privacy or data security program, but did not include monetary payments.[24]

c. Eleventh Circuit Issues Important Decision in LabMD Case

As we highlighted in last year's Review, a now-defunct medical lab company, LabMD, last year appealed an FTC order finding that the company failed to reasonably protect its customers' personal information from data breaches and requiring implementation of a comprehensive information security program to prevent future breaches. This long-running case has been one of the highest-profile FTC data security enforcement actions, testing the boundaries of the FTC's authority. The company, in pursuing the litigation, has argued forcefully that the FTC overstepped its enforcement authority because, among other reasons, no consumer was injured as a result of the data breach.[25]

In June 2018, the Court of Appeals for the Eleventh Circuit issued an important decision that held the FTC's cease-and-desist order, which directed the company to implement a variety of security measures, was unenforceable.[26] In the decision, the court assumed, *arguendo*, that the company's "negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a)," and therefore did not reach the question of whether consumers had been injured.[27] Nonetheless, the court held that even assuming the behavior was an unfair act or practice, the FTC's order failed to enjoin any *specific* act or practice.[28] Instead, the Court held that the FTC's order inappropriately required the company "to overhaul and replace its data security program to meet an indeterminable standard of reasonableness," requiring the Court to vacate the order.[29]

By calling into question the FTC's ability to fashion an enforceable order in data security cases, the Eleventh Circuit decision puts the burden on the FTC to define more clearly the conduct it is challenging and the remedies it seeks. Going forward, we will be watching carefully to see how the FTC structures its orders to navigate these issues.

2. Department of Health and Human Services and HIPAA

Despite operating with a lower budget in 2018 than in previous years, the Department of Health and Human Services ("HHS") has continued its strong efforts to enforce patient privacy violations, including imposing its largest ever fine to date, while also considering major regulatory overhauls to the Health Insurance Portability and Accountability Act ("HIPAA") regulations. But HHS is not the only entity

seeking to enforce healthcare privacy violations, as 2018 also saw the first multi-state data breach lawsuit brought by Attorneys General of several states alleging violations of HIPAA. These developments are addressed below.

a. HHS OCR Enforcement

There were several notable HIPAA-related settlements and judgments during 2018:

Health Insurer. In October 2018, a large health insurer agreed to pay HHS's Office for Civil Rights ("OCR") $16 million and take "substantial corrective action" in response to alleged HIPAA violations related to a series of cyber-attacks in 2015, whereby hackers obtained electronic protected health information ("ePHI") relating to more than 79 million individuals.[30] The settlement almost tripled the previous high water mark for HIPAA enforcement settlements, which was set in 2016 and matched in 2017.[31] OCR justified its high settlement by alleging that the insurer "failed to implement appropriate measures for detecting hackers who had gained access to their system to harvest passwords and steal people's private information."[32] The insurer had allegedly "failed to conduct an enterprise-wide risk analysis, had insufficient procedures to regularly review information system activity, failed to identify and respond to suspected or known security incidents, and failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI."[33] Taken together, these alleged violations and the seriousness of data breaches in the healthcare space led HHS to seek the high settlement.

Dialysis Provider. In February 2018, HHS reached a $3.5 million settlement with a national dialysis provider following a series of five separate breach reports alleging incidents that occurred in 2012 at five different locations.[34] Emphasizing the need for performing risk assessments and risk analysis, HHS indicated that the "number of breaches, involving a variety of locations and vulnerabilities, highlights why there is no substitute for an enterprise-wide risk analysis for a covered entity."[35]

Cancer Center. In June 2018, in a case that was not settled, an HHS Administrative Law Judge ("ALJ") ruled against a hospital-based cancer center, finding on summary judgment that the cancer center had violated HIPAA following the theft or loss of a laptop and two USB thumb drives containing unencrypted ePHI in 2012 and 2013, and assessed a $4.3 million penalty.[36] Key to the ALJ's ruling was the center's purported failure to address its risk assessment findings related to encryption. Specifically, the ALJ found evidence that the center knew about the high risk to ePHI since at least 2006, stemming from the potential use of unencrypted devices, but failed to implement remediation until 2011, and even then did so inadequately.[37]

Medical Records Company. In February 2018, HHS OCR entered into a settlement that serves as a reminder that a covered entity's obligations under HIPAA do not end when the company goes out of business, when it agreed to a $100,000 settlement with a now-bankrupt medical records storage company.[38] Even after the company went out of business as part of an unrelated litigation, HHS alleged that the company had allowed an unauthorized individual to transport PHI, and declared that the "careless handling of PHI is never acceptable," agreeing to take the settlement out of the liquidated assets designated for distribution to creditors and others.[39]

b. Request for Public Comments on Reforming HIPAA

In addition to bringing enforcement actions, HHS also initiated a far-ranging review of HIPAA regulations, including asking for public comments on how it can amend HIPAA to "remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and to promote the transformation to value-based healthcare, while preserving the privacy and security of PHI."[40] The request for comments includes 54 questions, and interested parties must submit comments by February 12, 2019.

c. State AGs Bring Multi-State Action Premised on HIPAA

Outside of HHS—in the first ever multi-state data breach lawsuit alleging violations of HIPAA—twelve state Attorneys General,[41] led by Indiana Attorney General Curtis T. Hill Jr., filed a complaint in Indiana federal court against a healthcare information technology company and its subsidiary related to a breach discovered in 2015 that compromised personal data of 3.9 million people.[42] Notably, the lawsuit alleges that the company failed to protect ePHI in the hands of its business associate after a breach related to a third-party web application run by the company.[43] The case was filed in December, 2018, and Gibson Dunn will continue to monitor developments.

d. HHS Issues Guidance on Cybersecurity Practices for the Healthcare Industry

In late December 2018, HHS released detailed guidance on cybersecurity practices in the healthcare space.[44] The publication was the result of a public-private taskforce that formed under a legislative mandate to develop practical and cost-effective cybersecurity guidelines.[45] While adoption of the practices outlined in the guidance is voluntary, informed implementation could supplement an effort to demonstrate reasonable care in a negligence case related to cybersecurity, while failure to do so could lead to allegations of failure to take reasonable care. The guidance includes two technical volumes—one for small organizations and one for medium and large organizations—that are organized under the 10 "most effective" cybersecurity practices as identified by the task force.[46] These practices are not intended to be exhaustive or applicable to every entity, and the document encourages tailoring cybersecurity controls to the specific healthcare entity.[47]

3. Securities and Exchange Commission

As anticipated, the Securities and Exchange Commission ("SEC") devoted increased attention in 2018 to cybersecurity enforcement and to regulatory activity, particularly around cryptocurrency and initial coin offerings.

a. Cybersecurity and Data Breaches

SEC Guidance. In February 2018, the SEC announced new guidance to assist public companies in understanding their disclosure obligations with respect to cybersecurity risks and incidents and to highlight the importance of cybersecurity policies and procedures.[48] The guidance was the SEC's first major pronouncement on these issues since 2011,[49] and the new guidance "reinforce[es] and expand[s]

the previous guidance," including by emphasizing "the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context."

Insider Trading Charges. In March and June 2018, the SEC charged two employees of a credit reporting agency with insider trading in advance of the company's September 2017 disclosure of a data breach affecting nearly 150 million people. Specifically, the SEC charged the credit agency's former Chief Information Officer, and a former manager.[50] The manager was charged after he deduced that a website for an unnamed client affected by the breach was in fact for consumers of the credit reporting agency.[51] The charges underscore the importance of implementing internal policies and controls to prevent trading on non-public information related to cybersecurity incidents, and the personal risk to executives who make trades without disclosing such information first.

Internal Accounting Controls. In October 2018, the SEC issued a report cautioning public companies about the importance of internal controls to prevent cyber fraud. The report described the SEC Enforcement Division's investigation into whether nine unidentified companies that were victims of cyber-related fraud had sufficient internal accounting controls in place to satisfy their obligations under Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934. The SEC ultimately decided not to pursue enforcement actions against the nine companies, but advised issuers and other market participants to consider cyber-related threats when devising and maintaining a system of internal accounting controls.[52] The report points to the SEC's growing interest in corporate controls designed to mitigate cyber risks, and should be understood as a warning to public companies that future investigations could lead to enforcement actions.[53]

b. Cryptocurrency

In addition to regulatory efforts by other financial industry actors such as the Federal Reserve, the Commodity Futures Trading Commission, the Federal Deposit Insurance Commission, and state agencies, the SEC made regulation of cryptocurrencies and protection of investors from the risks associated with investment in digital assets a major focus in 2018.

In January 2018, the SEC filed a complaint against a cryptocurrency platform[54] and obtained a court order halting an allegedly fraudulent initial coin offering ("ICO"). For the first time in connection with an ICO, the court approved a receiver to secure various cryptocurrencies held by the platform.[55]

SEC Chairman Jay Clayton later testified before Congress, noting that the SEC monitors cryptocurrency-related activities of brokers, dealers, investment advisers, and other market participants it regulates. Clayton advised that ICO market participants should assess whether a coin or token is a security and, if a cryptocurrency is a security, must comply with the registration and other requirements of the federal securities laws.[56]

4. Other Federal Agencies

Although not as active or far reaching as actions by the FTC, HHS, or the SEC, other federal agencies also continue to make headlines in the data security and privacy space. This year in particular, there

were notable developments at the Federal Communications Commission ("FCC"), Consumer Financial Protection Bureau ("CFPB"), and Department of Defense ("DoD").

a. Federal Communications Commission

i. FCC Robocall Initiative

The FCC and FTC joined together to host two events aimed at preventing illegal robocalls and caller ID spoofing.[57] The agencies hosted a Policy Forum in March 2018 to discuss the challenges posed by robocalls and the efforts being taken by both agencies to protect consumers. The agencies also hosted a Technology Expo for consumers in April 2018, featuring technologies, devices, and applications to curb illegal robocalls.[58] In announcing the events, leaders of both agencies highlighted the invasion of privacy consumers experience when receiving robocalls and the prevalence of consumer complaints on the issue.[59]

ii. ACA Int'l v. FCC

As discussed in further detail in Section II.C. below, in March 2018, the D.C. Circuit issued a ruling that changes the rules for what constitutes an auto-dialer.[60] The court held that the FCC's use of the phrase "automatic telephone dialing system"—as interpreted in the FCC's 2015 omnibus Declaratory Ruling and Order (the "omnibus order")—was unreasonably broad under the Administrative Procedure Act ("APA") because it effectively encompassed any uninvited call or message from any smartphone, due to smartphones' potential to randomly dial numbers if a downloaded app could provide it such capabilities.[61] The court also set aside as arbitrary and capricious the omnibus order's imposition of liability for calling reassigned numbers without prior consent, even if the consent had been given by the number's previous holder.[62] The court upheld the omnibus order's conclusion that "a called party may revoke consent at any time and through any reasonable means"—orally or in writing—"that clearly expresses a desire not to receive further messages."[63] In its decision, the court noted that the FCC was working to develop a new regime to avoid the reassignment issues involved in *ACA International*.[64] As discussed below, the FCC approved new reassignment rules in June 2018.

iii. FCC Rulemaking

Slamming and Cramming. In June 2018, the FCC approved new rules relating to "slamming," the unauthorized change of a consumer's preferred telephone company, and "cramming," imposing unauthorized charges on a consumer's phone bill.[65] The rule prevents phone companies from using deceptive tactics to obtain verification from consumers to switch service providers.[66] Under the new rule, material misrepresentations will invalidate any alleged authorization given by a consumer to switch providers.[67] Phone companies may face a five-year suspension from using third-party verification procedures for abusive practices.[68]

Reassigned Numbers Database. In December 2018, the FCC adopted new rules to establish a reassigned numbers database.[69] The rule will address unwanted calls to consumers caused by consumers who get a new phone and receive a reassigned number.[70] Previously, businesses and other callers would call the consumer, looking for the holder of the number and not realizing the number had been

reassigned.[71] The rule establishes a single, comprehensive database with information provided by phone companies—and for callers who use the database, the rule will provide a safe harbor from liability for any calls to reassigned numbers caused by database error.[72]

b. Consumer Financial Protection Bureau

In December 2018, the Senate confirmed Kathy Kraninger as director of the CFPB.[73] Kraninger's appointment follows a contentious battle between Trump appointee Mick Mulvaney, a critic of the agency, and deputy director Leandra English, who both claimed to be the lawful acting chief of the bureau.[74] During her first day, Kraninger indicated a desire to distance herself from Mulvaney's approach and promised that the agency "absolutely will take the enforcement actions to the full extent of the law and make sure we are protecting consumers."[75] Kraninger also stated that a priority is examining the bureau's measures to secure the consumer data it collects.[76]

The CFPB's own security measures were called into question toward the end of 2017 after reports of a data breach, and the CFPB subsequently implemented a freeze on the collection of personally identifiable information ("PII").[77] In May 2018, however, acting director Mick Mulvaney lifted the freeze after an independent review concluded that the CFPB's cybersecurity defenses were secure.[78]

Given the changes in leadership, and Mulvaney's efforts to scale back enforcement efforts, it is no surprise that the CFPB was not active in the enforcement area during 2018. In the wake of the data breach at a major credit reporting agency in 2017, for example, the company initially disclosed in its SEC filings that the CFPB was investigating the company. Since then, conflicting reports have claimed that Mulvaney declined to issue subpoenas or schedule interviews with the company's leadership, even though the probe remains open.[79]

c. Department of Defense

Defense Department Cyber Strategy. In September 2018, the DoD issued a Cyber Strategy report outlining the DOD's "vision for addressing this threat and implementing the priorities of the *National Security Strategy* and *National Defense Strategy* for cyberspace."[80] The report identified key cyberspace objectives of the department,[81] and explained that to achieve these goals, DoD will focus on developing cyber capabilities for warfighting and countering malicious cyber-attacks.[82] This includes a focus on strengthening relationships with the private sector with advanced cyber capabilities to leverage the skills, resources, capabilities, and perspectives of those outside DOD.[83]

"Do Not Buy" List For Foreign Software Vendors. In July 2018, the DoD announced its creation, with the help of the intelligence community, of a "do not buy" list for defense suppliers.[84] The list identifies certain vendors whose software originates in Russia or China, with the aim of helping the industry "steer clear of potentially problematic" products, those which "don't operate in a way consistent" with defense standards.[85] The "do not buy" list is part of a larger effort by the federal government to prevent Russian and Chinese penetration into defense and industrial systems.[86]

5. State Attorneys General

State Attorneys General continued to play a key role in data privacy and security matters this past year, acting at the forefront of concerted efforts to bring enforcement actions and regulate the technology industry.

a. Collaboration Among Attorneys General

In 2018, states continued the trend of coordinating enforcement efforts with each other to settle multi-state litigations involving large-scale data breaches. For example, as discussed above, in December 2018, eleven Attorneys General filed a federal complaint in the Northern District of Indiana against an electronic medical records company for violating provisions of HIPAA and state data and consumer protection laws when hackers stole protected health information relating to millions of individuals. The suit marks the first time Attorneys General joined to file an action stemming from a HIPAA-related data breach in federal court.[87]

b. Developments Within States

In May 2018, the New Jersey Attorney General announced plans to create a Data Privacy & Cybersecurity ("DPC") Section within his office, under the authority of the Affirmative Civil Enforcement Practice Group, in response to increasing threats to online privacy.[88] The DPC Section will take over the work of privacy and data security investigations and litigation from the Office's Consumer Fraud Prosecution section.[89]

Also in May 2018, the New Jersey Attorney General, in partnership with New Jersey's Division of Consumer Affairs, entered into settlement with a Chinese app developer resolving the Division's investigation into allegations that the company violated COPPA and the New Jersey Consumer Fraud Act ("CFA") by collecting information from children under the age of 13 without parental consent.[90] The developer agreed to pay $100,000 in fines and change its apps to prevent the collection of children's data.[91]

In June 2018, the New York Attorney General announced that several major business and consumer organizations endorsed the office's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") of 2017. The Act would require companies to adopt "reasonable" safeguards for sensitive data and expand the categories of data triggering reporting requirements.[92] The Attorney General concurrently released a "Small Business Guide to Cybersecurity in New York State,"[93] which offers advice to small businesses on how to secure sensitive data and respond to data breaches.

In September 2018, the New Mexico Attorney General filed suit against several mobile app developers for allegedly collecting personal data from children under the age of 13 without parental consent in violation of COPPA as well as of state law.[94] The Attorney General expressed concerns that such data collection creates the "unacceptable risk of data breach and access from third parties" who may "exploit and harm" children.[95]

In December 2018, the D.C. Attorney General filed a lawsuit against Facebook alleging that the company allowed Cambridge Analytica to gain access to information on D.C. residents for use in targeted ad campaigns during the 2016 presidential election.[96] The Attorney General's complaint alleges violations of the District's Consumer Protection Procedures Act.[97]

6. New York Department of Financial Services

The New York Department of Financial Services ("NYDFS") is the most active state cybersecurity regulator in the nation. As noted in last year's Review, New York's Cybersecurity Regulation, 23 NYCRR 500, proposed by NYDFS in September 2016, became effective March 1, 2017, and marks a sweeping effort to impose cybersecurity obligations on a broad set of regulated institutions.[98]

Specifically, 23 NYCRR 500 applies to all entities licensed or otherwise regulated by NYDFS, including state-chartered banks, licensed lenders, private bankers, foreign banks licensed to operate in New York, mortgage companies, insurance companies, and, by extension, service providers to such regulated entities ("Covered Entities").[99]

All Covered Entities were already required:

- By August 2017, to designate a Chief Information Security Officer; implement an overall cybersecurity program and appropriate cybersecurity policies; regulate access privileges; develop an incident response plan; and be able to notify the Superintendent of Financial Services within 72 hours of a cybersecurity incident;

- By March 2018, to conduct a risk assessment; implement cybersecurity monitoring, testing, and personnel training; maintain effective controls, such as multi-factor authentication; and have the Chief Information Security Officer prepare a written report to the board of directors; and

- By September 2018, to develop and periodically update policies and procedures to secure in-house and externally developed applications; detect unauthorized access to, use of, or tampering with nonpublic information; and to implement limits on data retention, audit trails to detect and respond to cybersecurity incidents, and controls, such as encryption, to protect nonpublic information.[100]

For certain of the above measures, the board of directors or a senior officer of the company must certify that the company is in compliance by next month, February 15, 2019.[101]

In addition, by March 1, 2019, the final transitional compliance deadline, Covered Entities must ensure that the third-party vendors with whom they do business also have adequate cybersecurity policies. Specifically, Section 500.11 requires Covered Entities to "implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers," including "relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers."[102]

The Superintendent of the Department of Financial Services, Maria T. Vullo, announced that the Department will incorporate cybersecurity in all of its regulatory examinations, including adding cybersecurity-related questions to "first day letters" (i.e., notices the Department issues to launch examinations of financial services companies).[103]

The Department has also ventured into an enforcement role. In June 2018, the Department, along with seven other state regulatory agencies, entered into a consent order with a national credit reporting agency stemming from its 2017 data breach. Although the order does not impose a fine, it requires the agency to develop a risk assessment, establish a formal internal audit program, and improve board oversight of information security, vendor management, patch management, and information technology operations.[104]

Additionally, on July 3, 2018, the Department adopted a new regulation, 23 NYCRR 201.07, requiring consumer credit reporting agencies ("CCRAs") to register with the Department and to comply with the cybersecurity regulations under 23 NYCRR 500, with a final deadline of December 31, 2019, to comply with all requirements, including section 500.11.[105]

Other states are expected to follow suit in enacting similar cybersecurity regulations.[106]

B. LEGISLATIVE DEVELOPMENTS

1. Federal Legislative Developments

2018 saw a flurry of congressional activity in the area of cybersecurity, particularly compared to 2017. The most significant piece of privacy legislation to be signed into law was the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") (*see* Section III.B.). In addition, Congress reauthorized Section 702 of the Foreign Intelligence Surveillance Act (*see* Section III.C.) and took steps towards addressing cybersecurity, data privacy, and robocalling, though few of those bills have become law.

a. Enacted Legislation

i. The CLOUD Act

As discussed further in Section III.B. below, on March 23, 2018, Congress passed, and President Trump signed into law, the CLOUD Act,[107] which amends the Stored Communications Act of 1986 ("SCA")[108] to allow the federal government to obtain warrants to compel service providers to turn over customer data stored outside of the United States and enter into bilateral data-sharing agreements with foreign governments for law enforcement purposes. Service providers would be permitted to move to quash warrants obtained by the government if there is a material risk that compliance with the request would violate the laws of a foreign government.[109] As discussed further in Section III.B., the legislation stemmed from litigation between the federal government and a prominent tech company that had reached the U.S. Supreme Court.[110]

The CLOUD Act was supported by several tech giants who argued that it appropriately balances individual privacy rights and would help reduce international disputes.[111] Other activist

organizations, on the other hand, expressed concern that it does not provide sufficient procedural protections for cross-border access to consumer information.[112]

ii. Foreign Surveillance

As discussed further in Section III.C. below, in January 2018, Congress reauthorized Section 702 of FISA for another six years without any significant changes.[113] Section 702 allows the government to collect foreign communications without a warrant; however, the reauthorization does require the FBI to obtain a court order based on probable cause to access the communications of U.S. persons in criminal investigations unrelated to national security.[114] Additionally, the reauthorization resumes the controversial "abouts" collection program, which allows the government to collect communications that contain a reference to a target (i.e., communications "about" a target), instead of just communications to or from a target, pending written notice to Congress.[115]

b. Proposed Legislation

i. TRACED Act

On November 15, 2018, Senators John Thune (R-SD) and Edward Markey (D-MA) introduced the Telephone Robocall Abuse Criminal Enforcement and Deterrence ("TRACED") Act,[116] which would amend the Communications Act of 1934 to authorize the FCC to crack down on illegal robocalls by creating authentication rules for voice service providers to prevent "caller ID spoofing."[117] The bill provides for significant penalties against telemarketers and scammers that use automatic dialing services, imposing a $10,000 fine for each call made in intentional violation of the law,[118] and increases the statute of limitations (to three years, up from one) for the FCC to bring an action against violators.[119] It also brings together various federal agencies, state Attorneys General, and other non-federal entities to report to Congress on improving enforcement measures and directs the FCC to promulgate rules designed to stop texts and calls made using unauthenticated numbers.[120] There has been no additional action on the bill in 2019.

ii. Cybersecurity and Data Breach Notification

There was little agreement in Congress this year over how to respond to data breaches such as the breach of a prominent consumer credit reporting agency in 2017. On December 11, 2018, Republican and Democratic leaders on the House Oversight Committee released dueling reports responding to that breach, with the Democratic report chastising House Republicans for not demanding stricter cybersecurity laws.[121] The Democratic report recommended increasing financial penalties for data breaches, strengthening the FTC's enforcement authority over credit agencies, and passing legislation that would create a framework for notifying victims of data breaches.[122] In contrast, the Republican report suggested forming more public-private partnerships, requiring credit reporting agencies to be more transparent with consumers, and providing a "government-wide framework of cybersecurity and data security risk-based requirements" for federal contractors.[123]

The proposed Consumer Privacy Protection Act of 2017,[124] which was introduced by Senator Mark Warner (D-VA) at the end of that year and would require disclosure of security breaches and

implementation of comprehensive consumer privacy and data security programs by certain commercial entities, did not appear to make any headway in 2018. Its future in the new Congress is uncertain.

iii. Email Collection by Law Enforcement

As discussed further in Section III.A. below, efforts to reform the Electronic Communications Privacy Act ("ECPA") fell short in 2018, despite advocacy from the technology industry and privacy organizations. Controversially, ECPA still allows the government to obtain a court order (not a search warrant) directing service providers to grant access to emails after 180 days have passed.[125] In 2018, the House passed the Email Privacy Act ("EPA") as part of the Fiscal Year 2019 National Defense Authorization Act ("NDAA") to impose a warrant requirement for access to emails over 180 days old.[126] As in 2017, the bill lost steam in the Senate, where the final version of the NDAA passed without EPA's reforms or the broader ECPA Modernization Act of 2017 introduced by Senators Mike Lee (R-UT) and Patrick Leahy (D-VT) last year.[127]

2. State Legislative Developments

In 2018, states continued to supplement federal law with their own data privacy regulations. The trend in state legislation has broadly been to tighten controls and provide higher levels of consumer protection, with some exceptions. California and New York have led the way with substantial data privacy and cybersecurity regulations implemented last year, and other states have enacted laws pertaining to data breaches, cybersecurity, and online privacy.

a. Data Breach Legislation

In 2018, Alabama and South Dakota joined the national trend of enacting data breach notification legislation, meaning that all 50 states (as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands) now have data breach notification laws in place.[128] The Alabama Data Breach Notification Act of 2018 generally requires entities to notify subjects of a breach involving their electronically stored "sensitive personally identifying information," which includes health information and other private details that could lead to access of sensitive data, no later than 45 days after learning of the beach.[129] South Dakota's data breach notification law provides a similar scope of protection, but requires notification within 60 days absent exceptional circumstances.[130] Other states, such as Louisiana, amended existing data breach notification laws with more detail regarding definitions, timelines, and data disposal in case of a breach.[131]

b. California Consumer Privacy Act of 2018

On June 28, 2018, California passed the California Consumer Privacy Act of 2018 ("CCPA"), which will broadly raise the bar for companies, regardless of where located, that handle the personal information of California consumers. The law is scheduled to go into effect on July 1, 2020 (or possibly later, see below)[132] and is projected to affect over 500,000 companies.[133] Taking a cue from the EU's General Data Protection Regulation ("GDPR"), the CCPA represents a much more comprehensive and stringent approach to data privacy than most existing privacy laws in the United States.

Since its passage, however, various concerns have been raised about the law, which was hastily enacted to prevent an even more onerous privacy initiative from being presented to voters on the November 2018 ballot.[134] Since its passage, the CCPA has been amended once, and further amendments are expected prior to its effective date.[135]

The CCPA requires businesses that collect personal information relating to California consumers to, among other things: (1) disclose what personal information is collected and the purposes for which that information is used; (2) delete a consumer's personal information if requested to do so, unless it is necessary for the business to maintain such information for certain purposes; (3) disclose what personal information is sold or shared and to whom; (4) stop selling a consumer's personal information if requested to do so (*i.e.*, the "right to opt out"), unless the consumer is under 16 years of age, in which case the business is required to obtain affirmative authorization to sell the consumer's information (*i.e.*, the "right to opt in"); and (5) not discriminate against a consumer for exercising any of the aforementioned rights, including by denying goods or services, charging different prices, or providing a different level or quality of goods or services, subject to certain exceptions.[136]

With one exception, the CCPA does not include a private right of action, and thus the law will largely be enforced by the California Attorney General (as opposed to consumers filing private lawsuits). The exception is that consumers whose non-encrypted or unredacted personal information has been accessed, exfiltrated, stolen, or disclosed "as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" may initiate a civil lawsuit.[137]

The Attorney General has until July 2020 to develop and publish rules implementing regulations for the CCPA and cannot enforce them until the later of July 1, 2020 or six months after their publication.[138] Therefore, enforcement cannot begin until at least July 2020, and possibly later.

For a detailed discussion of the original Act, see our July 12, 2018 client alert. For a discussion of the September amendments, see our October 5, 2018 client alert.

c. Other California Legislation

In September 2018, California also passed an expansive law regulating "connected devices," broadly applying to *any* devices with the *ability* to connect to the internet and that are assigned an Internet Protocol ("IP") or Bluetooth address.[139] The law requires that every connected device must have a "reasonable security feature" that is: "(1) Appropriate to the nature and function of the device. (2) Appropriate to the information it may collect, contain, or transmit. (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."[140]

The law does not specify what a reasonable security feature entails, except that it does indicate that a connected device has a reasonable security feature if it is "equipped with a means for authentication outside a local area network" with a "preprogrammed password [] unique to each device manufactured" or "contains a security feature that requires a user to generate a new means of authentication before

access is granted to the device for the first time."[141] Outside of this caveat, future enforcement actions will likely detail the specific guidelines for this regulation.

d. Other Cybersecurity Legislation

Ten states also enacted legislation in 2018 relating to consumers requesting security freezes on their credit reports.[142] These statutes largely require credit reporting agencies to honor consumers' requests to freeze their credit reports without charging a fee, in order to facilitate further security in case of data breaches.

But not every legislative action has afforded heightened consumer protection. For example, effective November 2, 2018, Ohio enacted a "safe harbor" provision that allows businesses that have established written cybersecurity programs that meet industry standard requirements to claim an affirmative defense against tort claims alleging a failure to implement reasonable security controls.[143] The law notably does not impose liability on businesses that fail to meet the standard; rather, it can only be used as an affirmative defense.[144]

II. CIVIL LITIGATION

A. PRIVACY LITIGATION

1. Class Action Litigation

a. High-Profile Incidents and Related Litigation in 2018

In 2018, there were numerous attacks on technology, hospitality, retail, healthcare and other companies that exposed personal data and resulted in litigation.

i. Technology Companies

Social Media Network. On March 17, 2018, the *New York Times* reported that British political consulting firm Cambridge Analytica had obtained information on more than 50 million users of Facebook.[145] Shareholders brought several derivative lawsuits that were consolidated in the Northern District of California, and the social media network's motion to dismiss is currently pending before the court.[146] A number of consumer class action were also consolidated in the Northern District of California. At the end of December 2018, the social media network filed its reply in support of its motion to dismiss, which contends, among other arguments, that the plaintiffs have not suffered any actual or concrete harm.[147]

Social Media Network. In October 2018, Google announced that it was shutting down its social network following a report by the *Wall Street Journal* that a bug had exposed the profiles of hundreds of thousands of users for three years.[148] On December 10, 2018, the company disclosed another bug that had exposed the profile data of 52.5 million users, including data such as name, age, email address, and occupation.[149] The company now faces a class action complaint in the Northern District of

California,[150] and several shareholder lawsuits in New York and California federal courts, including one brought by an investment fund owned by the state of Rhode Island.[151]

ii. Political Breaches

Russia's alleged interference with the 2016 presidential election continued to draw attention throughout the year. On May 8, 2018, the Senate Intelligence Committee released a briefing that concluded Russia was engaged in efforts to undermine the integrity of the 2016 elections.[152] It stated that Russian hackers had breached the security of election computers in several states and were "in a position to" alter voter registration data. There was ultimately, however, no evidence that Russia actually changed vote tallies or the registration information of voters.[153] On July 13, 2018, the U.S. Department of Justice indicted twelve Russian intelligence officers for hacking the systems of the Democratic Congressional Campaign Committee, the Democratic National Committee ("DNC"), and Hillary Clinton's presidential campaign, as well as for conspiring to hack state boards of elections and U.S. companies that supplied election software.[154]

On April 20, 2018, the DNC brought suit against the Russian government, Donald J. Trump for President, Inc., and Wikileaks in a New York federal court. The complaint asserts that the defendants conspired to hack the Democratic Party in order to benefit President Trump's campaign, including by illegally accessing the DNC's emails, donor information, opposition research, and strategic plans.[155] On December 10, 2018, Donald J. Trump for President, Inc. and Wikileaks moved to dismiss the suit on First Amendment grounds, and for failure to adequately state a claim.[156]

iii. Consumer Information

International Hotel Management Company. On November 30, 2018, an international hotel management company announced a data breach that potentially exposed information on approximately 300 million guests.[157] Following the announcement, consumers filed putative class actions in Maryland, Illinois, Massachusetts, California, and New York.[158] A shareholder also brought suit in a New York federal court.[159]

Sports Apparel Company. On March 30, 2018, a fitness apparel brand announced that an "unauthorized party" had acquired account information, including usernames, email addresses, and hashed passwords, for around 150 million users of its fitness-tracking app.[160] The hacker did not gain access to payment card data because the company stored that information separately.[161] In the wake of the disclosure, an app user initiated a class action lawsuit, and the company is currently seeking to arbitrate the matter.[162]

Department Stores. On April 2, 2018, the owner of two national department stores announced an attack affecting potentially five million customers.[163] Hacker group JokerStash Syndicate claimed that they stole five million credit card and debit card numbers and had been releasing them for sale on the dark web.[164] JokerStash has been linked to several past breaches, including those of a national grocery chain and fast casual restaurant chain.[165] Consumers filed several class actions in the wake of the April announcement, including in New York, California, Delaware, and Tennessee federal

courts.[166] On August 1, 2018, the Judicial Panel on Multidistrict Litigation rejected a request by one of the plaintiffs to centralize the lawsuits in New York.[167]

On April 4, 2018, a separate department store revealed that a cyberattack on its online customer service vendor exposed the payment information of 100,000 customers.[168] An airline company also used the same vendor and estimated that the incident may have affected several hundred thousand of its customers as well.[169] Consumers filed at least one class action lawsuit following the announcement.[170]

And after a data breach left consumer data exposed from April to June 2018, a customer of another large department store brought a complaint in an Alabama federal court alleging that the company failed to adequately protect consumer data such as names, addresses, and credit card numbers.[171]

iv. Healthcare Data

Breaches of healthcare data have been rising for years, according to a study of annual health data breaches, and 2018 was no different.[172] On July 30, 2018, a hospital health system suffered a phishing attack that impacted the records of 1.4 million patients.[173] Some of the healthcare provider's employees had transmitted their login credentials in response to an email that falsely appeared to be from a company executive.[174] The attack exposed information such as patient names, dates of birth, medical and treatment information, lab results, social security numbers, driver's license numbers, insurance information, and payment information.[175] This was the second successful phishing attack on the hospital in 2018.[176] The first breach affected 16,000 patients.[177] The hospital group faces a class action in Wisconsin federal court and has moved to dismiss the matter on the theory that the plaintiffs did not properly plead traceable harm.[178]

Other healthcare providers also suffered data breaches that exposed the patient data of more than 500,000 patients each.[179]

b. Update on High-Profile Data Breach Cases from Prior Years

i. District Court Litigation

Consumer Credit Reporting Agency. A consumer credit reporting agency faced a series of lawsuits following a hack of its computer system in 2017 that exposed the names, social security numbers, addresses, and other PII of more than 140 million people.[180] On December 6, 2017, the class actions were consolidated in the Northern District of Georgia.[181] Since then, the agency has been fighting to dismiss various parts of the cases. On July 17, 2018, the agency moved to dismiss dozens of banks and credit unions' claims on standing grounds, arguing that the financial institutions had not adequately alleged that any fraudulent charges had been made on payment cards they had issued.[182] And on July 30, 2018, the agency moved to dismiss small business plaintiffs on standing grounds as well, arguing that businesses cannot bring claims arising from injuries that their owners allegedly suffered.[183] On December 14, 2018, the court heard oral argument on the motion to dismiss the consumer, financial institution, and small business plaintiffs.[184]

Restaurant Chain. A restaurant chain faced lawsuits by financial institutions as a result of a 2017 data breach that affected its payment card data.[185] On October 24, 2018, the federal court in Colorado dismissed the majority of the claims, including those under negligence and trade secret law.[186] The court allowed the counts under California's unfair competition law, New Hampshire's consumer protection law, and tort law to proceed.[187]

ii. Appellate Litigation

Federal Agency. In 2017, the District Court for the District of Columbia dismissed a class action suit filed after the Office of Personnel Management ("OPM") suffered a breach that affected the data of past and present U.S. government employees.[188] In May 2018, various groups, including federal employee unions and privacy organizations, urged the D.C. Circuit to revive the litigation.[189] The groups disagreed with the district court's finding that the plaintiffs had not pleaded an actual injury and lacked Article III standing.[190] On November 2, 2018, the D.C. Circuit heard oral argument, and the parties are awaiting a decision.[191]

Health Insurance. In 2017, the D.C. Circuit ruled that members of a Maryland insurer could proceed with a class action lawsuit alleging that their personal information was stolen in a 2014 data breach.[192] The parties disputed whether plaintiffs had sufficient Article III standing based on a substantial risk of *non*-imminent future harm.[193] On February 20, 2018, the Supreme Court denied without comment the company's petition for certiorari, which would have been the first data breach case to reach the Supreme Court.[194] In its petition, the company had argued that Supreme Court guidance was necessary to resolve a circuit split over whether the exposure of personal data satisfied the standing requirement.[195]

Online Retailer. On March 8, 2018, the Ninth Circuit revived a class action filed in response to a 2012 data breach that affected the data of 24 million online shoppers.[196] The panel ruled that the plaintiffs had adequately shown standing because of the sensitivity of the information exposed, credit card numbers, and risk of identity theft, phishing, and pharming.[197] On August 20, 2018, the retailer filed a petition for certiorari and urged the Supreme Court to resolve a circuit split over whether exposure to a data breach constitutes an injury under Article III.[198]

National Bookstore. On April 11, 2018, the Seventh Circuit revived a proposed class action alleging that a large bookstore failed to secure customers' financial data during a 2012 security breach.[199] The panel held the customers adequately pleaded injuries, which included money spent on credit-monitoring services and time spent "to set things straight."[200] The panel sent the proceedings back to the lower court to adjudicate the merits and decide whether the proposed class should be certified.[201]

c. Circuit Split on Standing in Post-*Spokeo* 2018

Following the Supreme Court's decision in *Spokeo, Inc. v. Robins*,[202] circuits continue to be split over how to satisfy the Article III standing requirement in data breach cases. The D.C. Circuit in *Attias v. CareFirst Inc.* found that the mere exposure of personal information and risk of identity theft are sufficient to demonstrate standing.[203] CareFirst filed a petition for certiorari, arguing that the circuit split was ripe for clarification; on February 16, 2018, the Supreme Court denied certiorari.[204]

The Ninth Circuit also ruled in *In re Zappos* that victims of a data breach adequately pleaded standing because the information exposed in the data breach (credit card numbers) was sensitive, and because stolen data could be used to harm the plaintiffs.[205] The Ninth Circuit reasoned that *Clapper v. Amnesty International* was not applicable because that case involved a challenge to surveillance procedures authorized by the Foreign Intelligence Surveillance Act, and thus involved a more speculative threat of identity theft and unique national security concerns.[206] Zappos subsequently submitted a petition for certiorari, and it remains to be seen whether the high court will take up the case.[207] The petition was distributed on November 20, 2018, which suggests that the Court may come to a decision soon.

By contrast, the Second, Fourth, and Eighth Circuits have found that the risk of identity theft or credit card fraud does not constitute a concrete harm.[208]

d. Shareholder Derivative Suits

Data privacy incidents typically spark both class actions brought by consumers (like those discussed above), as well as by shareholders. This year was no different.

First, a restaurant chain settled a derivative action pending in the Southern District of Ohio brought by certain shareholders before there was even a consolidated complaint and before the court had assessed who to appoint as lead counsel.[209] The lawsuit stems from the company's disclosure that malware had affected the company's point-of-sale system, enabling credit card data to be stolen from 300 of its franchised restaurants.[210] The settlement agreement, which is currently pending approval by the district court, does not provide a payment of any funds, but instead would require the company to implement certain remedial cybersecurity measures to prevent future breaches.[211] Notably, the settlement provides for a newly created board-level Technology Committee with oversight over the company's cybersecurity and information technology, requires the company to maintain its advisory council of franchisee representatives, and requires the company to either provide certain foundational security services to its franchisees or designate an approved vendor for such services.[212]

In the wake of this settlement, two prominent class action securities fraud lawsuits were filed following data security incidents:

Technology Company. After Google announced on October 8, 2018, that a problem with its software had exposed the personal profile data, including names, e-mail addresses, birth dates, profile photos, places lived, occupation, and relationship status, of nearly half a million users, several shareholders filed a proposed class action for damages under the Securities Exchange Act.[213] The plaintiffs allege that by not disclosing the technical problem back in March 2018 when it was first discovered, and instead disclosing in October after reports in *The Wall Street Journal*, the company deceived investors and caused shares to be traded at inflated prices.[214] Once the court appoints a lead plaintiff and lead counsel, the parties will meet and confer regarding the filing or designation of an operative complaint.[215]

Education Materials and Service Provider. On September 25, 2018, a company providing educational materials and services to high school and college students announced that an unauthorized party had

gained access to the user data of approximately 40 million users, causing the company's share price to fall significantly. Days later, plaintiff shareholders filed a class action lawsuit in the Northern District of California against the company.[216] The complaint alleges that defendants' failure to disclose in its quarterly press release that it did not maintain sufficient data security measures constituted materially false or misleading statements and pointed to the fall in the company's share price following disclosure of a data breach to support its allegation that the share prices were artificially inflated by the conduct.[217] On December 10, 2018, the case was consolidated with a substantively similar putative class action complaint before Judge Charles Breyer of the Northern District of California, who will appoint a lead plaintiff and lead counsel.[218]

2. Settlements

In 2018, companies reached settlements over some of the largest data breaches on record. In addition, the Supreme Court considered the legality of the *cy pres* settlement at issue in a 2013 privacy class action against Google.

a. Health Insurer's Settlement

In 2015, a large health insurer announced that hackers had gained access to the names, birth dates, social security numbers, home addresses, and other personal information of approximately 79 million people.[219] In August 2017, the Northern District of California preliminarily approved a settlement of the numerous class action lawsuits brought by consumers.[220] On August 15, 2018, Judge Koh approved the settlement.[221] In a lengthy opinion, she determined that the settlement avoided the risk, expense, and duration of further litigation, and was an adequate amount when compared to other data breach settlements, and the damages calculation of the plaintiffs' expert.[222]

b. Consumer Credit Reporting Agency's Settlement

In September 2015, a mobile telecommunications company announced that 15 million customers' data had been hacked on databases belonging to a consumer credit reporting agency, which it uses to conduct its credit checks.[223] The breach compromised names, addresses, and dates of birth, and may have implicated social security and driver's license numbers.[224] The telecommunications customers brought suit against the credit reporting agency for claims of negligence, and 32 cases were consolidated in December 2015 in the Central District of California.[225] On November 12, 2018, the plaintiffs moved for preliminary approval of a $22 million settlement fund.[226] The settlement would also include credit monitoring services and an additional $11.7 million in remedial and enhanced security measures.[227]

c. Supreme Court's Review of a 2013 Cy Pres Award

During this term, the Supreme Court considered the legality of cy pres-only settlements, which provide no direct compensation to class members and instead distribute settlement proceeds to public interest organizations that further the interests served by the class action litigation. On October 31, 2018, the Supreme Court heard oral arguments regarding the legality of a 2013 settlement for a privacy class action that claimed a large technology company shared users' search queries with website owners.[228] Per

the settlement terms, of the $8.5 million settlement amount, $5,000 would go to three named plaintiffs, $2.15 million to class counsel, and $5.3 million to various internet privacy non-profit organizations.[229] The Competitive Enterprise Institution, a conservative think tank, argued that the settlement violated Federal Rule of Civil Procedure 23(e), which requires that class action settlements be "fair, reasonable, and adequate."[230]

During arguments, Justices Sotomayor and Breyer seemed to suggest the current system was working, as courts rarely approve cy pres-only settlements. Justices Roberts, Alito, and Kavanaugh expressed doubt at whether distributions to cy pres beneficiaries, who often had connections to class counsel rather than the class members, actually constituted relief.[231] Several justices also queried whether the plaintiffs had standing to bring the class action in the first place.[232] In a rare move, the Court responded by ordering the parties to brief the issue following oral arguments.[233] A decision on the matter is forthcoming.

d. Comparison of Settlements of Data Breach Claims from 2015-2018

To place this year's settlements in historical context, below are details of a number of significant settlements over the past few years.

Defendant Category	**Approval**	**Data Type**	**Relief to the Class**	**Service Awards, Fees, & Costs**
Health Insurer[234]	August 15, 2018	Personal Information	$115 million for, among other things, class members' out-of-pocket expenses and credit monitoring services; security practice changes	Up to $3 million in costs and $37.95 million in fees, to be covered by $115 million settlement payment
Home Improvement Retailer (Financial Institution Class)[235]	September 22, 2017	Card Data	$25 million for class claims; up to $2.25 million to certain sponsored entities; security practice changes	Up to $2,500 for each class representative; $710,000 in litigation costs; $15.3 million in fees
Home Improvement Retailer (Consumer Class)[236]	August 23, 2016	Card Data	Up to $13 million for class claims; up to $6.5 million for 18 months of credit monitoring services; security practices changes	$1,000 for each representative plaintiff; $166,925 in costs; $7.536 million in fees

Defendant Category	Approval	Data Type	Relief to the Class	Service Awards, Fees, & Costs
Department Store (Financial Institution Class)[237]	May 12, 2016	Card Data	Up to $20.25 million for class claims; $19.108 million to MasterCard; Reportedly up to $67 million for Visa's claims against Target[238]	$20,000 for 5 representative plaintiffs; $2.109 million in costs; $17.8 million in fees
Entertainment Company[239]	April 6, 2016	Login and Personal Information	Up to $2 million for preventative losses; up to $2.5 million for claims for identity theft losses; up to two years of credit monitoring services	$3,000 for each named plaintiff; $1,000 for each plaintiff who initially filed an action; $2.588 million in fees
Healthcare Services Company[240]	February 3, 2016	Health Information	$7.5 million in cash payment; up to $3 million for class claims; one year of credit monitoring services (offered during remediation); security practice changes	$50,000 in incentive payments for class representatives; $7.45 million in fees and costs
Department Store (Consumer Class)[241]	November 17, 2015	Card Data	Up to $10 million for claims; security practice changes	$1,000 for three deposed plaintiffs; $500 for other plaintiffs; $6.75 million in fees
Social Networking Service[242]	September 15, 2015	Login Information	Up to $1.25 million for claims; security practice changes	$5,000 for the named plaintiff; $26,609 in costs; $312,500 in fees
Computer Software Company[243]	August 13, 2015 Voluntary Dismissal	Login and Card Data	Security practice changes and audit	$5,000 to each individual plaintiff; $1.18 million in fees

Defendant Category	Approval	Data Type	Relief to the Class	Service Awards, Fees, & Costs
Entertainment Company[244]	May 4, 2015	Card Data and Personal Information	Up to $1 million for identity theft losses; benefit options including free games and themes or month subscription, unused wallet credits, virtual currency; some small cash payments	$2.75 million in fees

B. INTERCEPTIONS AND EAVESDROPPING

1. Email Scanning

This year, compared to 2017, saw fewer developments in class action lawsuits alleging technology companies violated state and federal laws by scanning user emails. Nonetheless, companies operating electronic communications services should continue to monitor such lawsuits, as they concern potentially massive proposed classes including all or many users of such services.

Email Web Service. On June 6, 2018, a web service that unsubscribes users from mailing lists, newsletters, and other unwanted emails prevailed on consent grounds in its motion to dismiss claims under the ECPA, the SCA, and California's Invasion of Privacy Act ("CIPA").[245] The plaintiffs asserted that the web service intercepted and accessed users' emails without consent or authorization, or exceeded authorization by accessing emails for the purpose of extracting and selling consumer data.[246] The court noted that "[a]ll of the Complaint's statutory claims depend on a lack of consent."[247] Plaintiffs alleged that they consented for the web service "to access their emails only for the limited purpose of cleaning up their inboxes, and that they did not allow [the company] to sell their data for market research purposes."[248] But the court rejected this proposition because "the privacy policy reserves the right to do exactly what [the company] did: 'collect and use your commercial transactional messages and associated data to build anonymous market research products and services with trusted business partners.'"[249]

2. Call Recording

In recent years, there have been a number of civil and criminal cases brought against both businesses and individuals for recording phone calls without the requisite consent. The recording of telephone conversations is governed by a patchwork of federal and state law. At the federal level, the Wiretap Act permits the recording of phone calls, so long as one party to the call consents to the recording.[250] The vast majority of states have similarly adopted a "one-party" consent requirement, while a minority of states have adopted either a "two-party" or "all-party" consent requirement. Most of the call recording cases brought in recent years have been against companies for large-scale recordings of commercial calls, rather than individual illicit recordings.

Although nearly a dozen states have all-party consent laws, lawsuits for call recording under the CIPA continue to expand.[251] The growing trend of recording of employee and customer calls for a number of quality assurance purposes combined with ongoing notice and consent issues ensures that this will be an evergreen target for lawsuits. Furthermore, in 2016, the U.S. District Courts for the Southern District of California and Central District of California determined that non-California plaintiffs may assert CIPA claims against California defendants where the alleged violations occurred in California.[252] These developments escalate potential liability risk and encourage business to remain attentive.

Banking Institution. On July 10, 2018, the Western District of Pennsylvania determined that the plaintiff had alleged sufficient facts to establish claims for intentional interception of a wire communication and for invasion of privacy under Pennsylvania common law, denying the bank's motion to dismiss.[253] Plaintiff alleges that the bank used an automated system to make and record over 35 debt collection calls to his cellular phone without his consent or any prior business relationship.[254] Each call made plaintiff aware that recording would occur, but the court (noting Pennsylvania's longstanding two-party consent rule) was not persuaded by an implied or implicit consent theory because "Plaintiff was a party to multiple telephone calls in which he actively exchanged words with Defendant; accordingly, his consent was required to record the calls," but instead "[Plaintiff] explicitly declined to consent to interception of his calls by Defendant."[255]

Banking Institution. On January 16, 2018, a California Court of Appeals reversed summary judgment granted to a large bank for CIPA call recording claims brought by a mother of an employee.[256] Plaintiff alleged that the bank recorded 316 phone calls between her, her daughter, and one with her daughter's coworkers on an company phone line.[257] The employer's "Electronic Monitoring and Device Use" policy authorized its employees to use company telephones for personal calls and expressly warned that their "personal calls may be recorded."[258] The employer argued that "it did not 'intentionally'—for purposes of sections 632(a) and 632.7(a)—record" and that "'the mere act of [an employer] installing a recording device on company phones and 'by chance' recording non-work related calls between [Rojas] and [her d]aughter does not satisfy the 'intentional' requirement of [s]ections 632 and 632.7.'"[259] The Court of Appeals disagreed, citing guidance from the California Supreme Court: "the recording of a confidential conversation is intentional if the person using the recording equipment does so with the purpose or desire of recording a confidential conversation, or with the knowledge to a substantial certainty that his use of the equipment will result in the recordation of a confidential conversation."[260] Under this standard, the court determined that the employer failed to meet its burden of showing that it lacked the requisite intent.[261]

3. Other "Interceptions"

In the Internet of Things ("IoT") age, new technologies allow for new forms of surreptitious recording and tracking. This year saw a number of developments including new, creative theories of Wiretap Act violations.

Television Manufacturer. On October 4, 2018, defendant television manufacturer entered into a settlement agreement in response to a putative class action in the Central District of California.[262] In the original lawsuit, plaintiffs alleged that the company violated the ECPA and the Video Privacy and

Protection Act ("VPPA"), as well as several state law fraud, negligent misrepresentation, and consumer protection claims.[263] Plaintiffs alleged that the defendant used smart TVs to secretly collect, and distribute to advertisers, information on customer viewing habits so that advertisers could deliver targeted advertising in real time.[264] Plaintiff's second consolidated complaint alleged that the television software took samples of the programming displayed at any point in time and sent "fingerprints" of those samples to the centralized matching server to compare against already existing fingerprints in the database, a process that operates sufficiently fast to provide "at least some context-sensitive content substantially simultaneously with at least one targeted video."[265] The October 4, 2018 settlement agreement requires the defendant to pay a $17 million settlement and take several additional steps to remedy the situation (including changing its disclosures for new customers, and adding a disclosure to the guide that accompanies new TV purchases).[266]

Mattress Company, Men's Retailer, and Outdoor Retailer. On July 12, 2018, a mattress company, a men's clothing company, and an active outdoor retailer faced allegations of using certain software to de-anonymize online users and "observe their keystrokes, mouse clicks, and communications with the e-commerce retailers' websites."[267] The plaintiff, alleging the code functions as a "wiretap," brought a putative class action in the Southern District of New York, alleging that the use of such software was a violation of the Wiretap Act, ECPA, as well as the SCA and New York's General Business Law.[268] But the defendants prevailed on a motion to dismiss. The court determined that the plaintiffs' Wiretap Act claims fail "because § 2511 is a one-party consent statute . . . . [and i]t is clear that the Retailers were parties to the communications and [the defendant] had their consent."[269] The plaintiff's ECPA claims failed because "there is no private cause of action under § 2512."[270] The SCA claims failed for insufficient pleadings: the plaintiff "offers nothing more than 'labels and conclusions' that the communications were held in electronic storage."[271]

Mortgage Lender. On November 9, 2018, a mortgage lender faced a similar lawsuit (with the addition of a common law intrusion upon seclusion claim) for allegedly using similar de-anonymizing and keylogging software.[272] Again, the defendant prevailed on a motion to dismiss because the plaintiff "admit[ed] that any allegedly intercepted communications were made on" the company's website, making the defendant "a party to the communication."[273] The court dismissed without prejudice the plaintiff's state common-law tort of intrusion upon seclusion claim because "it appears that [the plaintiff] might be able to allege sufficient facts for this Court to exercise original jurisdiction over his intrusion upon seclusion claim."[274]

C. TELEPHONE CONSUMER PROTECTION ACT

As in past years, 2018 included several notable actions and developments under the Telephone Consumer Protection Act ("TCPA").[275]

The highlight came in March, when the D.C. Circuit published its long-anticipated opinion in *ACA International v. FCC*.[276] That case interpreted the FCC's 2015 omnibus Declaratory Ruling and order (the "omnibus order") which, among other things, defined what qualifies as an "automatic telephone dialing system" ("ATDS").[277] The applicable statute defines ATDS as "equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number

generator; and (B) to dial such numbers."[278] The D.C. Circuit vacated two of the omnibus order's interpretations of this definition:

First, *ACA International* held the omnibus order unreasonably defined "capacity." Under the omnibus order, whether equipment has the "capacity" to qualify as an ATDS turns on the equipment's *potential* functionality, rather than its *current* capabilities. In concluding this definition was unreasonable, the court emphasized that "any smartphone, with the addition of software, can gain the statutorily enumerated features of an autodialer."[279] Accordingly, if a device's "capacity" under the TCPA turns on its potentiality, then "under the Commission's approach" "all smartphones . . . meet the statutory definition of an autodialer"—an "untenable" result.[280]

Second, *ACA International* vacated the omnibus order's definitions of when a device can (1) "store or produce telephone numbers to be called, using a random or sequential number generator" and (2) "dial such numbers,"[281] because the omnibus order failed to make clear how a device meets these two requirements. In some places, "the order convey[ed] that equipment needs to have the ability to generate random or sequential numbers that it can then dial" to meet these requirements.[282] But other times, the order suggested "equipment c[ould] meet the statutory definition even if it lacks that capacity."[283] Though the court acknowledged it "might be permissible for the Commission to adopt either interpretation," endorsing these competing contentions at the same time fell below the bar of reasoned decision-making.[284]

In the months since *ACA International*, courts have started to grapple with important questions left unanswered by the decision. In particular, there is an emerging circuit split over what functionality a device must have in order to qualify as an ATDS.

In *Dominguez v. Yahoo*, the Third Circuit concluded a device that sent text messages to phone numbers *manually entered into* the system did not qualify as an ATDS.[285] This was because the system did not have the "present capacity to function as an autodialer by generating random or sequential telephone numbers and dialing those numbers."[286] *Dominguez* thus stands for the proposition that a device can *only* qualify as an ATDS under the Act when the device has the present capacity to place calls to randomly generated or sequential numbers.[287]

The Ninth Circuit, in contrast, defined ATDS far more broadly in *Marks v. Crunch San Diego*.[288] That case centered on a web-based marketing platform designed to send promotional text messages to a list of stored telephone numbers.[289] Relying on the context and structure of TCPA, the court held that a device that calls a stored list of numbers—rather than numbers generated randomly or sequentially—could, in fact, qualify as an ATDS.[290] In so doing, the court relied on two aspects of the TCPA: (1) the fact that, in other provisions, the Act allowed an ATDS to call selected numbers, and (2) that when Congress amended the statute, it did not amend the definition of an ATDS, even though under the amended statute "equipment that dial[ed] from a list of individuals who owe a debt to the United States" was, in fact, an ATDS, although it was exempted from the TCPA.[291]

The FCC has taken notice of these decisions. On May 14, 2018, the FCC sought public comments on the open questions that *ACA International* raised.[292] And just a few months after that, on October 3,

2018, the FCC issued another notice seeking public comments on the TCPA's definition of ATDS in light of *Marks v. Crunch San Diego*.[293] We expect the FCC may publish a new order interpreting this TCPA issue sometime in 2019.

Related to FCC interpretation of the law, the Supreme Court recently granted the petition for certiorari in *PDR Network v. Cartlon & Harris Chiropractic*, a case that raises important questions about a 2006 FCC Rule interpreting the term "unsolicited advertisement."[294] The district court concluded that it need not defer to and apply the 2006 Rule because it unambiguously contradicted the statute.[295] The Fourth Circuit reversed the decision. It held that *Chevron*'s deferential framework[296] did not apply in this context because the Hobbs Act grants the D.C. Circuit *exclusive* jurisdiction to enjoin, set aside, suspend and determine the validity of "FCC interpretations of the TCPA."[297] It follows, the Fourth Circuit reasoned, that it (and every circuit besides the D.C. Circuit) lacks jurisdiction to set aside FCC's interpretations of the Act and, instead, must defer to them.[298] Nevertheless, on November 13, 2018, the Supreme Court granted a petition for a writ of certiorari on the following question: Whether the Hobbs Act required the district court in this case to accept the FCC's legal interpretation of the TCPA.[299] The argument date has not yet been set.

Finally, Congress has also taken a keen interest in the TCPA. Indeed, both the House and the Senate are considering new legislation that would amend TCPA. The Stopping Bad Robocalls Act, introduced in the House by Congressman Frank Pallone Jr. and in the Senate by Senator Edward J. Markey, would replace the definition of ATDS with "robocall."[300] This new definition would explicitly cover devices that make calls using "numbers stored on a list."[301] Similarly, Massachusetts Senator Ed Markey and South Dakota Senator John Thune introduced the TRACED Act in the Senate, which would (1) "broaden[] the authority of the FCC to levy civil penalties of up to $10,000 per call" for those "who intentionally flout telemarketing restrictions," and (2) extend the window for the FCC to take civil enforcement action against intentional violations up to three years after a robocall is placed, instead of one year.[302] We will be watching carefully whether either of these bills gain traction.

D. VIDEO PRIVACY PROTECTION ACT

Compared to the TCPA, there were relatively few significant developments in 2018 regarding the VPPA.

In fact, one of the only notable decisions on VPPA this year was a district court decision in *White v. Samsung Electronics America*, which followed binding Third Circuit precedent and dismissed the plaintiff's claim that smart TVs violated the VPPA because the TVs "monitor[ed] and track[ed] consumers viewing habits and record[ed] consumers' voices" and "then transmit[ed] that information."[303] The court based its decision on the fact that, in the Third Circuit, data points such as IP address, MAC address and WiFi access point do not qualify as PII. And since the data the smart TVs allegedly recorded was "the same type of static digital identifiers the Third Circuit ha[d] determined" did not constitute PII, the court dismissed the complaint.[304]

In last year's Review, we also discussed certain circuits' (namely, the First, Third, and Ninth circuits') approach to the scope of PII, which the Act defines as including "information which identifies a person as having requested or obtained specific video materials or services from a video tape service

provider."[305] This year, no additional circuits considered the definition of PII in the context of the VPPA, but we expect that other circuits will do so in coming years.

E. BIOMETRIC INFORMATION PRIVACY ACTS

The biometric technology space also was active this year. As corporations and institutions increasingly incorporate the use of biometric information in their technologies and operations, states have raced to craft policies protecting the privacy rights of their residents.

The prevalence of these issues was frequently in the headlines. For example, earlier this year, the iconic Madison Square Garden began using facial recognition technology to enhance its security by cross-referencing the faces of individuals entering the stadium with photographs in a database of individuals who have caused security issues in the past.[306] Similarly, news broke in mid-December that Taylor Swift is using facial recognition at her concerts to identify stalkers.[307] And a major credit card company introduced new technology that allows users to scan their fingerprints onto a biometric card from their homes.[308] The saved fingerprint scan obviates the need for users to remember their PIN or provide a signature to authenticate transactions; users need only their thumbs.

In light of increasing use, and the sensitivity of these data—such data cannot be changed after all, unlike a password—several states have enacted biometric information privacy acts ("BIPAs"). Illinois, Texas, and Washington were the first, and most recently, California enacted the Consumer Privacy Act of 2018 ("CCPA")—discussed further in Section I.B.2. above—which explicitly includes "biometric information" in its definition of "personal information."[309]

While Texas's and Washington's BIPAs do not confer a private right of action, leaving enforcement to the state Attorneys General (similar to the current version of the CCPA), Illinois's does.[310] As in past years, therefore, BIPA cases in Illinois were a source of active litigation, with at least thirteen cases actively litigated during 2018. Generally speaking, these cases were brought by either employees objecting to their employer's practice of collecting biometric information, or consumers objecting to companies doing the same. Many of the key conflicts this year were focused on constitutional or statutory standing, the latter of which the Illinois Supreme Court resolved just days ago.

Earlier in the year, in *Sekura v. Krishna Schaumburg Tan, Inc.*,[311] a tanning salon customer brought BIPA claims against the salon for collecting her fingerprints without allegedly providing the statutorily required disclosure concerning the salon's retention policy, and for allegedly disclosing her fingerprints to a third-party vendor.[312] Plaintiff initially survived the salon's motion to dismiss, but shortly thereafter, the Appellate Court of Illinois, Second District, held in 2017 in *Rosenbach v. Six Flags Entertainment Corporation*[313] that standing under the Act required an "injury or adverse effect" *in addition to* a violation of the Act. This caused the trial court to reconsider and grant dismissal.[314] Plaintiff appealed, but prior to the hearing, the U.S. District Court for the Northern District of Illinois held in *Dixon v. Washington and Jane Smith Community—Beverly*[315] that the disclosure of personal information to a third-party vendor constitutes an injury-in-fact, and therefore satisfies plaintiffs' standing burden under Article III. Because Plaintiff alleged just that, the Illinois Appellate Court reversed the dismissal and remanded the matter back to the trial court.[316]

The Illinois Supreme Court then weighed in on the *Rosenbach* case, determining that a plaintiff is "aggrieved" under BIPA and has statutory standing to sue, even without alleging an "actual injury or adverse effect."[317] The Court found that BIPA confers individuals with a substantive right to control their biometric information, and that no-injury BIPA violations are not merely "technicalities," but "real and significant" harms to important rights created by the legislature.[318] The Court also reasoned that the private right of action and remedies exist to prevent and deter violations of individuals' BIPA rights, and that requiring would-be plaintiffs to wait to sue until they have suffered "actual injury" would defeat these purposes of the statute.[319] Because the *Rosenbach* plaintiff alleged violations of his BIPA rights—Six Flags allegedly collected his fingerprints for use in a season pass without providing the statutorily mandated notices or publishing a data retention policy—the Supreme Court reversed the appellate court's contrary conclusion and remanded the case back to the trial court.

Rosenbach may not be the final word on BIPA's private right of action. This year the Illinois State Senate also will consider a bill narrowing the impact of Illinois's BIPA.[320] We will discuss any judicial or legislative BIPA developments in our next update.

F. INTERNET OF THINGS AND DEVICE HACKING

There have been a number of developments in the past year regarding connected devices—the Internet of Things ("IoT")—as the internet has become more widely accessible on consumer products. Indeed, it is estimated that 55 billion IoT devices will be in use worldwide by the year 2025.[321] Many of these recent developments have involved attempts by policymakers to mitigate cybersecurity risks associated with connected devices, though the ever-changing nature of these threats have created challenges for regulators.

1. Legislation

a. California Passes IoT Law

In September, California became the first state to pass a cybersecurity law requiring security features for "smart" devices and IoT-connected products.[322] On September 28, Governor Jerry Brown signed the two identical bills requiring manufacturers of connected devices to implement "reasonable security feature[s]" designed to protect the devices from unauthorized access.[323] Devices that are accessible outside of a local network will be in compliance with the law if they either (1) have a unique, preprogrammed password or (2) require users to generate a new means of authentication before they first use the device.[324] The bills require compliance by January 1, 2020 and exempt certain entities, like third-party software.[325] The bills do not create a private right of action for consumers.[326]

The legislation has received mixed reviews since its enactment. Some, like the California Manufacturers and Technology Association ("CMTA"), have characterized it as "[an] innovation-stifling measure[] [that] not only fail[s] to protect consumers, but will drive away California manufacturing investment."[327] Instead, the CMTA has recommended what it considers a fairer approach that "would ensure that all connected devices are compliant and secure, no matter where they are produced."[328] Similarly, Robert Graham, a security researcher, has criticized the law for "do[ing] little to improve security, while doing a lot to impose costs and harm innovation" because it requires

manufacturers to add costly security features, rather than removing *unsecure* features.[329] Others, like Bruce Schneier, Harvard University's "security guru," have lauded the bills for being a good first step in regulating a largely unregulated industry, saying, "[a] California law that manufacturers have to adhere to in California is going to help everybody."[330]

b. United States Congress Considers IoT Legislation

On November 28, the House of Representatives unanimously passed the SMART IoT Act, though the Senate did not pass the bill before the close of the 115th session of Congress. The Act would have required the Department of Commerce to conduct a study of the IoT industry in the United States, including identifying how the IoT is currently regulated, and submitting a report to Congress.[331]

In addition, Congress is currently considering the following legislation aimed at regulating the IoT:

- The Internet of Things Cybersecurity Improvement Act, which would require companies that transact with the federal government to ensure their IoT devices are patchable (i.e., able to be periodically upgraded), do not contain known vulnerabilities (or disclose known vulnerabilities), use standard network protocols, and do not contain hard-coded passwords;[332]
- The Securing the IoT Act, which would require the FCC to create cybersecurity standards for certifying wireless equipment;[333]
- The Developing Innovation and Growing the Internet of Things (DIGIT) Act, which would require the U.S. Secretary of Commerce to convene a "working group of Federal stakeholders" to create recommendations and a report to Congress on the IoT and the FCC to obtain public comments regarding spectrum needs relating to the IoT;[334]
- The Cyber Shield Act, which would create a voluntary labeling and grading system for IoT devices by requiring the Secretary of Commerce to establish a voluntary program to "identify and certify covered products with superior cybersecurity and data security through voluntary certification and labeling";[335] and
- The IoT Consumer Tips to Improve Personal Security Act, which would require the FTC to develop cybersecurity resources to educate consumers about the purchase and use of IoT devices.[336]

2. Regulatory Guidance

a. Consumer Product Safety Commission Holds Public Hearing on IoT and Product Safety Issues; FTC Issues Comment in Response

In May, the Consumer Product Safety Commission ("CPSC") received testimony from a variety of stakeholders at a public hearing regarding issues relating to IoT safety, and subsequently solicited comments from the public.[337] Among other things, the panelists highlighted the need to address product liability issues as well as privacy and security risks created by the IoT.[338]

Per the request of the CPSC during this effort, the FTC issued a comment in June on the topic.[339] The FTC advocated for flexible standards, suggesting "there is no 'one size fits all' approach to securing IoT devices," that companies should engage in periodic risk assessments evaluating their security programs, that IoT manufacturers should have oversight over service providers, and that products should be continuously updated and patched to meet evolving security threats.[340] The Commission also noted that its enforcement actions in the IoT space "send an important message to companies about the need to secure and protect internet-connected devices," and that the FTC "continues to devote substantial resources in this area . . . to foster competition and innovation in the IoT marketplace while protecting the safety of consumers."[341]

b. New FTC Commissioner Calls for More Robust Protections in IoT Space

In October, FTC Commissioner Rebecca Slaughter offered suggestions for strengthening protections in the IoT space in a speech at the Internet of Things Global Summit.[342] Slaughter noted that consumer trust in the IoT space includes both "ensuring that . . . devices are reasonably secure" and "ensuring that consumers have a clear and accurate picture of what data their devices collect and how that data is stored and used."[343] She also highlighted three common issues with IoT technologies that the FTC sees regularly: (1) "very basic failures in product design and pre-release testing"; (2) companies not foreseeing and addressing "credible alerts about potential vulnerabilities"; and (3) "challenges in the deployment of updates and patches."[344] Slaughter also advocated for federal privacy legislation similar to GDPR and California's CCPA that would provide the FTC with "rule-making authority, coupled with civil penalties in the areas of data security and privacy," and require the creation of a "Bureau of Technology" within the Commission to provide expertise in competition and consumer protection cases.[345]

3. Litigation

Connected Vehicles. In July, the Southern District of Illinois partially certified a class action against an automobile manufacturer, which alleges that several of the defendant's vehicles "suffer from potentially catastrophic design effects which allow third parties to remotely take control of the vehicles over the Internet while they are being driven."[346] Although the judge certified three state-based classes of drivers in Michigan, Illinois, and Missouri, he refused to certify a nationwide class of drivers, noting that doing so would require "highly individualized inquiries" to determine the underlying state law claims.[347] A trial has been scheduled for October 2019.[348]

Smart Home Devices. In October, a manufacturer of smart TVs agreed to settle a class action lawsuit claiming that it collected and sold its customers' viewing histories to third-party advertisers without their consent.[349] Per the settlement agreement, the company agreed to pay $17 million and to take additional measures to enhance its disclosures regarding data collection.[350] In the early days of January 2019, the court preliminarily approved the settlement.[351] The company had previously paid $2.2 million to the FTC and state of New Jersey in 2017 for similar allegations.[352]

G. COMPUTER FRAUD & ABUSE ACT

The Computer Fraud and Abuse Act ("CFAA") generally prohibits "access[ing] a computer without authorization or exceeding authorized access . . . ."[353] Because the CFAA does not clearly define either "authorized" or "access," courts have adopted disparate interpretations of these terms. The First, Fifth, Seventh, and Eleventh Circuits generally define these terms broadly, allowing liability both for access of digital information without authorization as well as improper use of information an individual was otherwise authorized to access.[354] Conversely, the Second, Fourth, and Ninth Circuits define the terms narrowly, allowing liability only where an individual accesses information without authorization.[355] Although the past year did not bring the circuits closer to harmony, it did include novel developments regarding the CFAA's application to employees accessing their employers' computers, and third parties accessing generally available websites in allegedly unauthorized ways.

Two cases in particular addressed whether an individual may be liable under the CFAA for allegedly misusing information he or she was otherwise authorized to access. The courts hearing these cases—applying the prevailing CFAA interpretations of their respective circuits—reached opposite conclusions. In *Teva Pharm. USA, Inc. v. Sandhu*, a pharmaceutical company alleged that a former employee had passed the company's trade secrets to the CEO of a competitor and filed suit against the former employee and others for CFAA violations, misappropriation of trade secrets, and various state law tort claims.[356] The U.S. District Court for the Eastern District of Pennsylvania denied in part Defendant's motion to dismiss, but granted dismissal for the company's CFAA claims. Because "[c]ourts within this district universally subscribe to the narrow approach, barring liability where the employee has authorization to access the computer to obtain the information,"[357] the Court held that "an employee who misuses information she was authorized to obtain cannot be held liable" under the CFAA.[358]

The U.S. District Court for the Northern District of Illinois took up similar questions in *Hill v. Lynn*.[359] The case centered on two co-founders of a software application company whose relationship had soured to the point that one co-founder, Lynn, cut off the other founder, Hill's, access to the company's email systems, downloaded source code Hill had created, and then deleted the code from the company's systems.[360] Hill sued Lynn for CFAA violations, fraud, and unjust enrichment, which Lynn moved to dismiss, arguing in part that she had not accessed the application's code "without authorization."[361] The Court granted the motion to dismiss in part, but denied it as to Hill's CFAA claims because, although "Lynn did have some kind of authorization to access the account," under Seventh Circuit precedent, "an employee who violates her fiduciary duty to her employer forfeits her authorization to access her employer's computers."[362] Taken together, *Sandhu* and *Hill* suggest that the United States Supreme Court may eventually have to decide how to interpret the CFAA as it applies to access to employers' digital information; but until then, companies should be on notice that the venue of any potential CFAA litigation may play an outsized role in the litigation's outcome.

This past year also saw courts applying the CFAA to third parties accessing generally available websites in potentially unauthorized ways, particularly through the use of computer "bots"—programs that access computers and websites to quickly acquire large quantities of information. Most notably, in *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, the online ticket vendor brought CFAA claims against

individuals who used bots to purchase large quantities of tickets through the site, in violation of the company's Terms of Use.[363] The Defendants filed a motion to dismiss, which the U.S. District Court for the Central District of California granted in part with respect to the company's CFAA claims. The Court noted that "a violation of the terms of use of a website—without more—cannot establish liability under the CFAA. However, a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly."[364] Because the company had not explicitly revoked users' permission to access its site, and instead had merely sent cease-and-desist letters, the Court ruled that it had failed to state a claim for relief, warranting dismissal. The company then amended its complaint, which the Court found to be sufficiently well-pled to survive dismissal because it alleged violations of the CFAA for "both access without authorization *and* situations where a defendant possesses some authorization, but acts in excess of that authorization."[365] Similarly, in *Sandvig v. Sessions*, the U.S. District Court for the District of Columbia adopted the "narrow interpretation" of the CFAA by ruling that a research team's plan to conduct studies using bots and fictitious online profiles would not violate the CFAA's authorization requirements.[366]

H. CYBERSECURITY INSURANCE

1. State of the Market

As predicted in last year's Review, the cybersecurity insurance market has continued to expand over the past year, with reports estimating a 25% growth rate.[367] While cyber-insurance penetration is around 30% for all businesses in the U.S., the rate is at an even higher 70% for Fortune 500 companies.[368] The value of the cyber insurance sector is currently estimated at $2 billion, but is expected to rise to about $10 to $15 billion in the next ten years.[369]

There are two primary reasons for the continued growth of the cyber-insurance market. First, large-scale and widely publicized hacks have convinced many companies of the costs and degree of business interruptions associated with cyber-attacks,[370] and an increase in cybercrimes has highlighted the importance of cyber-insurance.[371] Second, a growing regulatory regime governing data privacy and the resulting threats of fines and liabilities have encouraged businesses to purchase coverage.[372]

In response to growing demand, many insurers have expanded their cyber-insurance offerings,[373] including coverage for GDPR violations,[374] and have begun to offer a wide range of preventive services, such as phishing awareness campaigns, incident preparedness coaching, and regulatory readiness assessments.[375]

Although experts report that the industry is moving towards "all-risk" coverage,[376] insurers are cautious to proceed in the face of evolving risks, with some insurers limiting coverage to events triggered only by unauthorized activity or to costs that businesses must legally incur.[377] Other insurers are carefully evaluating companies' security practices when determining whether to provide coverage.[378] As demonstrated below, a mismatch of expectations over coverage has continued to trigger disputes between insurance companies and policy holders.[379]

2. State of the Law – Key Cases

a. Computer Fraud Insurance Provisions

In 2018, both the Second and Sixth Circuits ruled in favor of insurance policy holders, holding that computer fraud provisions contained in the companies' insurance agreements covered losses related to email-based "phishing" schemes.[380]

On July 6, 2018, the Second Circuit upheld the lower court's decision in *Medidata Solutions, Inc. v. Federal Insurance Co.*[381] As described in last year's Review, the company brought suit against its insurer to enforce their insurance agreement's computer fraud provision, which the company claimed covered "phishing activity," resulting from employees wiring $4.7 million to cybercriminals.[382] The district court determined that the policy provided coverage for the company's losses because the criminal activity was "deceitful and dishonest access."[383] The Second Circuit affirmed, reasoning that while "no hacking occurred," the cybercriminals "crafted a computer-based attack that manipulated the [plaintiff's] email system, which the parties do not dispute constitutes a 'computer system' within the meaning of the policy."[384] In reaching that decision, the Second Circuit distinguished a 2015 New York state court decision, *Universal American Corp.*,[385] reasoning that in that case, the court found lack of coverage because the fraud "only incidentally involved the use of computers,"[386] whereas in the instant case, the company's computer system *itself* was violated.[387] The Second Circuit also rejected the insurer's argument that the company failed to sustain a "direct loss" as a result of the attack, reasoning that the "spoofing attack was the proximate cause of [the company's] losses," because the attack initiated a "chain of events," which "unfolded rapidly," leading the company to transfer funds to the fraudsters the very same day.[388]

A week later, the Sixth Circuit released its decision in *American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America*, similarly siding with the policy holder when it reversed the lower court's decision and ruled that damages resulting from phishing activity was covered by the computer fraud provision of the company's insurance agreement. The district court had previously granted summary judgment for the insurer, reasoning that "[a]lthough fraudulent emails were used to impersonate a vendor and dupe [the plaintiff] into making a transfer of funds, such emails do not constitute the 'use of any computer to fraudulently cause a transfer.'"[389] The Sixth Circuit disagreed, reasoning that the fraudster's sending of emails to induce the transfer of money constituted "computer fraud" for the purposes of the insurance agreement because the fraudster used a computer to send these emails. The court continued that, if the insurance company wished to confine the definition of "computer fraud" to "hacking and similar behaviors," it could have done so.[390] The court also held that the fraudulent emails "directly caused" a "direct loss" to the insured company, because it precipitated a "chain of events," including a "series of internal actions," leading to the transfer of money to the fraudster.[391]

b. Commercial General Liability Insurance Policies

In 2018, the courts continued to grapple with coverage for data breach litigation costs. For example, in *St. Paul Fire & Marine Insurance Company v. Rosen Millennium, Inc.*,[392] the insurance company

filed a declaratory judgment action against its insured, a data security services provider, seeking a declaration that the insurer did not have to defend the security company against a suit by a hotel chain that alleged that the company's negligence caused a data breach potentially exposing the chain's customers' credit card information.[393] The insurer argued that the personal injury provision of the commercial general liability insurance ("CGL") policies—which provided coverage for, *inter alia*, "making known" a customer's credit card information—did not cover the breach at hand because the breach was perpetrated by a third party and "did not result from [the defendant's own] business activities."[394] The district court agreed,[395] finding the reasoning in *Innovak International, Inc. v. Hanover Insurance Company*[396] to be persuasive. There, the company's CGL policy similarly insured against the publication of "material that violates a person's right to privacy,"[397] and the court ruled that "the only plausible interpretation of the insurance policy is that it requires the insured to be the publisher of the private information," noting that "construing the policy to include the acts of third parties would be expanding coverage beyond what the insurance carriers were knowingly entering into."[398] Because the policy at issue in *St. Paul Fire* defined "personal injury" similarly to the policy in *Innovak*, the court in *St. Paul Fire* applied the same third-party perpetrator distinction.[399] Defendants in *St. Paul Fire* filed their notice of appeal and their brief is expected in mid-January 2019.[400]

c. Financial Institution Bonds

A third area of contention facing courts in 2018 was whether financial institution bonds cover losses resulting from data breaches. On June 28, 2018, a bank filed a complaint in the U.S. District Court for the Western District of Virginia against its insurer for failing to provide coverage for losses resulting from a data breach that exposed customer debit card information. The bank had claimed that the Computer & Electronic ("C&E") Crime Rider to the financial institution bond granted by the insurer covered the loss resulting from the breach.[401] The insurance company denied coverage under the C&E Crime Rider, arguing that the losses fell under the bond's Debit Card Rider, which maintained a significantly lower coverage limit.[402] In its complaint, the bank argued that the C&E Crime Rider controlled, because the criminal activity compromised the bank's systems, and the losses did not arise from the hackers' stealing debit card information directly from customers.[403] The insurer answered, raising a number of defenses based on the policy language, including the ability to deny coverage for losses resulting from "fraud or dishonesty of a natural person."[404] As with other cases regarding coverage of insurance policies for breach-related losses, the outcome of this case will likely be determined by extensive contract interpretation.

III. GOVERNMENT DATA COLLECTION

A. ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM

The ECPA,[405] passed in 1986 and amended in 1994, 2001, 2006, and 2008, was enacted to protect electronic information from unauthorized access.[406] The ECPA has three main provisions: Title I, the Wiretap Act, prohibits the interception and disclosure of another person's oral or electronic communications unless an exception applies, such as the government obtaining a court order authorizing surveillance.[407] Title II, the Stored Communications Act ("SCA"), protects from compelled

disclosure electronically stored information held by service providers;[408] and Title III authorizes the government to install devices, subject to a court order, that capture dialed numbers from placed calls, without intercepting the content of those calls.[409] To obtain a court order pursuant to Title III, the government must generally show that the information sought is relevant to an ongoing investigation.[410]

As briefly discussed above in Section I.B.1., there were two main efforts to reform the ECPA in 2018, only one of which was successful. On March 23, 2018, Congress passed, and President Trump signed, the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), which amended the SCA to allow the government to obtain a court order for customer data stored overseas.[411] Please see the Section III.B. for further discussion of the CLOUD Act.

The second reform effort this year, the Email Privacy Act ("EPA"),[412] failed to pass the Senate despite bipartisan support in the House of Representatives. The EPA—included as an amendment to the House's National Defense Authorization Act For Fiscal Year 2019 ("NDAA")[413]—would have codified the Sixth Circuit's 2010 decision in *United States v. Warshak* requiring law enforcement officials to obtain a warrant based on probable cause when seeking the content of email communications.[414] It also would have ended the ECPA's current "180-day rule," which allows the government to obtain email communications without a warrant after they have been held "in electronic storage" for more than 180 days.[415] A number of prominent technology companies and civil liberties groups publicly voiced their support for the bill in a July letter to the Senate and House Committees on Armed Services.[416] However, the EPA was not passed as part of the Senate's version of the NDAA and the House ultimately conceded during the conference committee process.[417] This represents the second time the EPA has failed to get through the Senate. In 2017, Senators Mike Lee (R-UT) and Patrick Leahy (D-VT) proposed the ECPA Modernization Act of 2017, which included the EPA and other reforms, but it was referred to the Senate Judiciary Committee and never received another vote.[418] With the newly Democratic-controlled House and Republican-controlled Senate, it is unclear what the future holds for the EPA or other reforms of the ECPA.

B. EXTRATERRITORIALITY OF SUBPOENAS AND WARRANTS AND THE CLOUD ACT

On October 16, 2017, the United States Supreme Court granted certiorari for review of *United States v. Microsoft Corporation*, which regards the scope of the government's power to obtain information stored overseas under the SCA.[419] The case involves Microsoft's challenge to a federal warrant seeking data stored at a Microsoft facility in Ireland.[420] Microsoft argued that the warrant was an inappropriate extraterritorial application of the SCA because the law's proper focus is on where electronic communications are stored, and that a search and seizure occurs in the jurisdiction of the storage.[421] The government, on the other hand, argued that the particular extraterritorial concerns should not be outcome determinative because the SCA's focus is on the disclosure of information, not storage.[422] During oral argument in February, the Court suggested that Congress may be the best arbiter and may update the law in response to this "brave new world" of extraterritorial data storage.[423]

In March, Congress passed the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") as part of the Consolidated Appropriations Act, 2018, Pub. L. 115–141. As briefly discussed above in Section I.B.1, The CLOUD Act amends the SCA by adding section 2713, which expands the geographic scope of the prior law by stating, in relevant part, that a "[service provider] shall . . . preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, *regardless of whether such communication, record, or other information is located within or outside of the United States*."[424] In response to the CLOUD Act, the Supreme Court issued a short per curiam opinion in *United States v. Microsoft Corp.* noting the mootness of the issue and vacating and remanding the case.[425]

To soften its broad reach, the CLOUD Act provides safeguards that limit the extraterritorial application to certain jurisdictions. Specifically, a motion to quash a subpoena for extraterritorial data may be granted if the required disclosure would cause the provider to violate the laws of a "qualifying foreign government."[426] Executive branch officials will determine which countries qualify based on several factors, including whether the foreign country has entered into an appropriate executive agreement, and whether the foreign country "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection . . . ."[427]

C. FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 REAUTHORIZATION

FISA[428] was passed in 1978, amended in 2008, and reauthorized for another six years in January 2018. As briefly discussed above in Section I.B.1., the purpose of FISA is to allow the U.S. government to acquire foreign intelligence information through electronic surveillance.[429] Foreign intelligence information is defined as information that allows the U.S. government to protect the country against hostile acts, sabotage or terrorism, or clandestine intelligence activities by a foreign power or agent.[430]

FISA established a specialized tribunal, the Foreign Intelligence Surveillance Court ("FISC"), to review the Attorney General's applications for authorization of electronic surveillance.[431] In 2017 (the most recent year for which data are available), the FISC received 1,614 applications, of which 1,147 were granted without any modification, 391 were granted with modification, and 76 were denied in full or in part.[432]

FISA Section 702, passed in 2008 as part of the FISA Amendments Act, authorizes the collection of communications from foreign persons reasonably believed to be located outside of the United States.[433] Critics of FISA, including Section 702, contend that the Act violates the First and Fourth Amendments of the Constitution by allowing law enforcement to sweep up communications passing through the United States, significantly increasing the scope of the government's surveillance power.[434]

Privacy advocates saw the pending reauthorization of FISA in late 2017 and early 2018 as an opportunity for reform, but those efforts were largely unsuccessful. The FISA Amendments Reauthorization Act of 2017—passed on January 18, 2018 and signed into law the next day—extends FISA for six years. It

reauthorizes the collection of not only those communications to or from the target of an investigation, but also those communications that simply contain a reference to a target, pending written notice to Congress that includes a FISC authorization of the program.[435] This is often referred to as "abouts" collection. One notable change, however, is a new requirement that the FBI obtain a court order based on probable cause to access the communications of U.S. persons in criminal investigations unrelated to national security.[436] FISA will next be subject to reauthorization at the end of 2023.[437]

D. COLLECTION OF CELLPHONE AND AUDIO DATA

This year, a number of court decisions addressed the issue of individuals' privacy rights with respect to cellphone and audio data. Although most of the decisions bolstered such rights by narrowing the government's ability to collect and search such data without a warrant, one Fourth Circuit case demonstrates that courts may be unwilling to curtail the government's ability to conduct warrantless searches pursuant to the border search exception.

1. Supreme Court Protects Cellphone Data in *Carpenter v. United States*

A key issue for the Supreme Court this past year was whether the government must obtain a warrant in order to collect an individual's cellphone site location history ("CSLI").[438] In *Carpenter v. United States*, the petitioner, an individual convicted of robbery, challenged the government's acquisition of several months' worth of CSLI, which identified the specific cell towers with which his phone connected while making and receiving calls.[439] On appeal, Carpenter, in conjunction with a number of individuals and entities who filed amici briefs, argued that the government violated his Fourth Amendment rights when it obtained the location records from his wireless carrier without a warrant.[440] In response, the government argued that, pursuant to the "third-party doctrine" established in the 1979 Supreme Court case *Smith v. Maryland*, individuals have no reasonable expectation of privacy in information they voluntarily surrender to third parties, including CSLI.[441]

The Supreme Court ruled in favor of the petitioner in a June 2018 decision authored by Chief Justice Roberts and joined by the Court's four liberal members.[442] The Court held that the Fourth Amendment requires the government to obtain a warrant to access CSLI, except in exigent circumstances.[443] In doing so, the Court reasoned that "[i]n light of the deeply revealing nature of CSLI, . . . the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[444] The Court also noted that individuals do not truly "share" CSLI with cellphone companies in the normal sense of the term because there is no "affirmative act on the part of the user."[445] The Court did note, however, that the decision was limited to the collection of historical CSLI covering an extended period of time, declining to consider whether the government would be allowed to collect information covering a shorter period of time without a warrant.[446] Further, the Court refused to overrule the third-party doctrine, instead emphasizing that CSLI is "qualitatively different" from other information the Court had previously allowed the government to obtain from third parties without a warrant (*e.g.*, telephone numbers, bank records).[447]

This decision continues the Supreme Court's trend in recent years of increasingly limiting the government's ability to access electronic personal information.[448] Companies that collect data from

users may now have a stronger basis for resisting requests made by law enforcement for CSLI without a warrant.

2. Massachusetts District Court Rules Fourth Amendment Protections Apply to Searches and Seizures of Cellphones at U.S. Border

On May 9, a federal district court in Massachusetts rejected the government's contention that Fourth Amendment protections do not apply to searches and seizures of cellphones at the U.S. border.[449] In *Alasaad v. Nielsen*, several U.S. citizens challenged the ability of federal officers at U.S. ports to search electronic devices without a warrant, contending that the government must have probable cause to suspect a violation of immigration or customs laws to do so.[450] The court agreed, rejecting the government's argument that the ruling in *Riley v. California*[451]—which requires a warrant for digital searches of cell phones incident to arrest—does not apply to the border search context, and instead reasoning that "the Supreme Court and First Circuit have acknowledged that digital searches are different too since they 'implicate privacy concerns far beyond those implicated' in a typical container search."[452]

3. Fourth Circuit Rules No Warrant Needed for Cellphone Border Probe

On May 18, the Fourth Circuit held that a "month-long, off-site forensic analysis" of a cellphone constituted a "nonroutine border search" and thus required some measure of individualized suspicion on the part of law enforcement officials.[453] The defendant in *United States v. Kolsuz* was a Turkish citizen detained at an airport after being charged with arms smuggling while attempting to board a flight to Turkey, at which point Customs and Border Protection officers took custody of his phone for several weeks to search its contents.[454] On appeal, the defendant argued that the district court erred by finding the probe to have been a "nonroutine border search justified by reasonable suspicion,"[455] arguing that the privacy interest in cellphones are substantial enough to require a warrant, even under the border exception.[456] The Fourth Circuit affirmed the district court's decision, ruling that the search was properly categorized as a border search; however, it declined to decide what measure of individualized suspicion was appropriate, even though the reasonable suspicion standard was met here, and instead concluded that agents' reasonable reliance on precedent was enough to preclude suppression.[457] The court described the border search exception as "broad enough to reach [this] search," despite the "temporal and spatial distance between the off-site analysis of the phone and the defendant's attempted departure at the airport."[458]

IV. CONCLUSION

We expect 2019 to be another significant year in the development and application of data privacy and cybersecurity law. As technology and data collection become more sophisticated, companies and governments will continue to explore the potential permissible uses of personal information. At the same time, the public will continue to debate the ideal balance between the benefits of big data and concerns for privacy and security. We will be tracking these important issues in the year ahead. Gibson Dunn is available to address any privacy or cyber concerns your business may face.

[1] Press Release, Federal Trade Commission, *Joseph Simons Sworn in as Chairman of the FTC* (May 1, 2018), https://www.ftc.gov/news-events/press-releases/2018/05/joseph-simons-sworn-chairman-ftc.

[2] *Id.*

[3] Press Release, Federal Trade Commission, *Phillips, Slaughter, and Chopra Sworn in as FTC Commissioners* (May 2, 2018), https://www.ftc.gov/news-events/press-releases/2018/05/phillips-slaughter-chopra-sworn-ftc-commissioners.

[4] Press Release, Federal Trade Commission, *Christine S. Wilson Sworn in as FTC Commissioner* (Sept. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/christine-s-wilson-sworn-ftc-commissioner.

[5] Press Release, Federal Trade Commission, *FTC Announces Sessions on Consumer Privacy and Data Security As Part of its Hearings on Competition and Consumer Protection in the 21st Century* (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its.

[6] Press Release, Federal Trade Commission, *Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act* (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] Press Release, Federal Trade Commission, *Mobile Phone Maker BLU Reaches Settlement with FTC over Deceptive Privacy and Data Security Claims*(Apr. 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/mobile-phone-maker-blu-reaches-settlement-ftc-over-deceptive.

[11] *Id.*

[12] *Id.*

[13] Decision and Order, *In the Matter of BLU Products, Inc.*, Docket No. C-4657 (F.T.C. Sept. 6, 2018), https://www.ftc.gov/system/files/documents/cases/172_3025_c4657_blu_decision_and_order_9-10-18.pdf.

[14] Press Release, Federal Trade Commission, *PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated*

Gramm-Leach-Bliley Act (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/05/ftc-gives-final-approval-settlement-paypal-related-allegations.

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] Press Release, Federal Trade Commission, *California Company Settles FTC Charges Related to Privacy Shield Participation* (July 2, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/california-company-settles-ftc-charges-related-privacy-shield.

[22] Press Release, Federal Trade Commission, *FTC Reaches Settlements with Four Companies That Falsely Claimed Participation in the EU-U.S. Privacy Shield* (Sept. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/ftc-reaches-settlements-four-companies-falsely-claimed.

[23] *Id.*

[24] Press Release, Federal Trade Commission, *California Company Settles FTC Charges Related to Privacy Shield Participation* (July 2, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/california-company-settles-ftc-charges-related-privacy-shield; Press Release, Federal Trade Commission, *FTC Reaches Settlements with Four Companies That Falsely Claimed Participation in the EU-U.S. Privacy Shield* (Sept. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/ftc-reaches-settlements-four-companies-falsely-claimed.

[25] *Id.*

[26] *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221, 1227 (11th Cir. 2018).

[27] *Id.* at 1237.

[28] *Id.* at 1236.

[29] *Id.*

[30] Press Release, Department of Health and Human Services, *Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History* (Oct. 15,

2018), *available at* https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] Press Release, Department of Health and Human Services, *Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules* (Feb. 1, 2018), *available at* https://www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html.

[35] *Id.*

[36] Press Release, Department of Health and Human Services, *Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations* (June 18, 2018), *available at* https://www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html.

[37] *Id.*

[38] Press Release, Department of Health and Human Services, *Consequences for HIPAA violations don't stop when a business closes* (Feb. 13, 2018), *available at* https://www.hhs.gov/about/news/2018/02/13/consequences-hipaa-violations-dont-stop-when-business-closes.html.

[39] *Id.*

[40] Request for Information on Modifying HIPAA Rules To Improve Coordinated Care, 83 Fed. Reg. 64302 (proposed Dec. 14, 2018) (to be codified at 45 C.F.R. pts. 160, 164), *available at* https://www.federalregister.gov/documents/2018/12/14/2018-27162/request-for-information-on-modifying-hipaa-rules-to-improve-coordinated-care.

[41] The states represented in this lawsuit are Arizona, Arkansas, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Nebraska, North Carolina, and Wisconsin.

[42] *See* Complaint, *State of Arizona v. Med. Informatics Eng'g, Inc.*, No. 3:18-cv-00969 (N.D. Ind. Dec. 04, 2018), ECF No. 1.

[43] *Id.*

[44] U.S. Dep't of Health & Human Servs. and Healthcare & Public Health Sector Coordinating Councils, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (Dec. 28, 2018), https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Press Release, Securities and Exchange Commission, *SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* (Feb. 21, 2018), https://www.sec.gov/news/press-release/2018-22; Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 C.F.R. pts. 229, 249, *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[49] *See* CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[50] *SEC v. Jun Ying*, No. 1:18-cv-01069-CAP (N.D. Ga. Mar. 14, 2018).

[51] *SEC v. Bonthu*, No. 1:18-cv-03114-MLB (N.D. Ga. June 28, 2018).

[52] Cyber-Related Frauds, Exchange Act Release No. 84429 (Oct. 16, 2018), *available at* https://www.sec.gov/litigation/investreport/34-84429.pdf.

[53] Gibson Dunn, *SEC Warns Public Companies on Cyber-Fraud Controls* (Oct. 17, 2018), https://www.gibsondunn.com/sec-warns-public-companies-on-cyber-fraud-controls/.

[54] Complaint, *SEC v. AriseBank*, No. 3-18CV-00186-M (N.D. Tex. Jan. 25, 2018), ECF No. 2, 2018 WL 623772; First Amended Complaint, *SEC v. AriseBank*, No. 3:18-cv-00186-M (N.D. Tex. Feb. 2, 2018), ECF No. 21, 2018 WL 1250524.

[55] Ex Parte Order Granting Emergency Ex Parte Motion for Temporary Restraining Order, *SEC v. AriseBank*, No. 3-18CV-00186 (N.D. Tex. Jan. 25, 2018), ECF No. 11; Press Release, Securities and Exchange Commission, *SEC Halts Alleged Initial Coin Offering Scam* (Jan. 30, 2018), https://www.sec.gov/news/press-release/2018-8.

[56] *Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC*, Testimony Before the Senate Committee on Banking, Housing, and Urban Affairs (Feb. 6, 2018), https://www.sec.gov/news/press-release/2018-8.

[57] Event, Federal Communications Commission, *Fighting the Scourge of Illegal Robocalls* (Mar. 23, 2018), https://www.fcc.gov/fcc-ftc-robocalls-forum.

[58] Event, Federal Communications Commission, *Stop Illegal Robocalls Expo* (Apr. 23, 2018), https://www.fcc.gov/news-events/events/2018/04/stop-illegal-robocalls-expo.

[59] Press Release, Federal Communications Commission, *FCC and FTC to Host Joint Policy Forum and Consumer Expo to Fight the Scourge of Illegal Robocalls* (Mar. 7, 2018),

https://www.ftc.gov/news-events/press-releases/2018/03/ftc-fcc-host-joint-policy-forum-consumer-expo-fight-scourge.

[60] *ACA Int'l v. Fed. Commc'ns Comm'n*, 885 F.3d 687 (D.C. Cir. 2018).

[61] *Id.* at 692-94.

[62] *Id.* at 692.

[63] *Id.* at 709.

[64] *Id.* at 709.

[65] Press Release, Federal Communications Commission, *FCC Adopts New Consumer Protections Against 'Slamming' and 'Cramming'* (June 7, 2018), https://www.fcc.gov/document/fcc-adopts-new-consumer-protections-against-slamming-and-cramming; FCC, Report and Order, Protecting Consumers from Unauthorized Carrier Changes and Related Unauthorized Charges, File No. 17-169 (June 7, 2018), https://docs.fcc.gov/public/attachments/FCC-18-78A1.pdf.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] Press Release, Federal Communications Commission, *FCC Establishes Reassigned Phone Numbers Database to Help Reduce Unwanted Calls to Consumers* (Dec. 12, 2018), https://docs.fcc.gov/public/attachments/DOC-355526A1.pdf; FCC, Order, Advanced Methods to Target and Eliminate Unlawful Robocalls, File No. 17-59 (Dec. 12, 2018), https://docs.fcc.gov/public/attachments/FCC-17-151A1.pdf.

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] Jim Puzzanghera, *New CFPB Director Kathy Kraninger says she won't be puppet of Mick Mulvaney*, Los Angeles Times (Dec. 11, 2018), http://www.latimes.com/business/la-fi-kathy-kraninger-cfpb-20181211-story.html.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] Lalita Clozel, *CFPB to Resume Private Consumer Data Collection*, Wall Street Journal, (May 31, 2018), https://www.wsj.com/articles/cfpb-to-resume-private-consumer-data-collection-1527796179.

[78] *Id.*

[79] Sylvan Lane, *Equifax says consumer bureau still probing hack despite report it eased off*, The Hill, (Mar. 2, 2018), https://thehill.com/policy/finance/376437-equifax-says-consumer-bureau-still-probing-hack-despite-report-it-eased-off.

[80] Department of Defense, Summary: Department of Defense Cyber Strategy 2018 (Sept. 18, 2018), *available at*https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[81] *Id.* at 3.

[82] *Id.* at 6.

[83] *Id.* at 7.

[84] Daniel Wilson, *DoD Making 'Do Not Buy' List for Foreign Software Vendors*, Law360, (July 27, 2018), https://www.law360.com/articles/1067768/dod-making-do-not-buy-list-for-foreign-software-vendors.

[85] *Id.*

[86] *Id.*

[87] Press Release, N.E. Attorney Gen., *Attorney General Files First Multi-State HIPAA-Related Data Breach Lawsuit* (Dec. 3, 2018), *available at*https://ago.nebraska.gov/news/attorney-general-files-first-multi-state-hipaa-related-data-breach-lawsuit.

[88] Press Release, State of N.J., Office of the Attorney Gen., *AG Grewal Announces Creation of New Enforcement Unit to Protect Data Privacy of New Jersey's Residents* (May 7, 2018), *available at* https://nj.gov/oag/newsreleases18/pr20180507b.html.

[89] State of N.J., Office of the Attorney Gen., *Data Privacy and Security*, https://www.nj.gov/oag/law/dpc.htm (last visited 12/19/18).

[90] N.J. Div. of Consumer Affairs, *NJ Division of Consumer Affairs Announces $100,000 Settlement with App Developer Resolving Investigation Into Alleged Violations of Children's Online Privacy Law* (May 8, 2018), *available at* https://www.njconsumeraffairs.gov/News/Pages/05082018.aspx.

[91] *Id.*

[92] Press Release, N.Y. State Office of the Attorney Gen., *A.G. Underwood Announces Broad Support for Shield Act from Major Business and Consumer Groups* (June 5, 2018), *available at* https://ag.ny.gov/press-release/ag-underwood-announces-broad-support-shield-act-major-business-and-consumer-groups.

[93] N.Y. State Office of the Attorney Gen., *Small Business Guide to Cybersecurity in New York State* (June 5, 2018), *available at*https://ag.ny.gov/sites/default/files/nyag_data_security_small_business_guide.pdf.

[94] Press Release, N.M. Attorney Gen, *AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data* (Sept. 12, 2018), *available at* https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location__Personal_Data_1.pdf;
Complaint, *Balderas v. Tiny Lab Productions et al.*, No. 1:2018-cv-00854 (D.N.M. Sept. 11, 2018).

[95] *Id.*

[96] Press Release, D.C. Office of the Attorney Gen., *AG Racine Sues Facebook for Failing to Protect Millions of Users' Data* (Dec. 19, 2018), *available at*https://oag.dc.gov/release/ag-racine-sues-facebook-failing-protect-millions.

[97] Complaint, *District of Columbia v. Facebook, Inc.*, No. 2018 CA 008715 (D.C. Super. Ct. Dec. 19, 2018).

[98] *See* 23 NYCRR 500, *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf; *see also, e.g.*, Gibson Dunn, *New York State Department of Financial Services Announces Proposed Cybersecurity Regulations* (Sept. 19, 2016), https://www.gibsondunn.com/new-york-state-department-of-financial-services-announces-proposed-cybersecurity-regulations/; Gibson Dunn, *New York State Department of Financial Services Revises Proposed Cybersecurity Regulations* (Jan. 5, 2017), https://www.gibsondunn.com/new-york-state-department-of-financial-services-revises-proposed-cybersecurity-regulations/.

[99] Nate Lord, *What Is the NYDFS Cybersecurity Regulation? A New Cybersecurity Compliance Requirement for Financial Institutions*, Digital Guardian (Sept. 19, 2018), https://digitalguardian.com/blog/what-nydfs-cybersecurity-regulation-new-cybersecurity-compliance-requirement-financial.

[100] *See* Gibson Dunn, *New York State Department of Financial Services*, *supra* note 98.

[101] Covered Entities were required to submit a certificate of compliance by February 15, 2018 for the measures required to be completed by August 28, 2017.

[102] 23 NYCRR 500.11(a)-(b); Barry R. Temkin & Kenneth M. Labbate, *NY Department of Financial Services Cybersecurity Regulations: An Update*, New York Law Journal (June 28, 2018, 2:30 PM), https://www.law.com/newyorklawjournal/2018/06/28/062918ny_temkin2/.

[103] Press Release, N.Y. Dep't of Fin. Servs., *DFS Superintendent Vullo Issues Cybersecurity Filing Deadline Reminder* (Jan. 22, 2018), https://www.dfs.ny.gov/about/press/pr1801221.htm.

[104] Press Release, N.Y. Dep't of Fin. Servs., *DFS Takes Additional Action To Hold Equifax Accountable for Massive 2017 Data Breach* (June 27, 2018), https://www.dfs.ny.gov/about/press/pr1806271.htm.

[105] 23 NYCRR 201.07, *available at* https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf201txt.pdf.

[106] *More State Cybersecurity Regulation Ahead for Financial Services Industry?*, LexisNexis State Net Capitol Journal (Mar. 8, 2018), https://www.lexisnexis.com/communities/state-net/b/capitol-journal/archive/2018/03/08/more-state-cybersecurity-regulation-ahead-for-financial-services-industry.aspx.

[107] Pub. L. 115-141 § 101 (2018).

[108] 18 U.S.C. § 2701, *et seq*.

[109] Pub. L. 115-141.

[110] *United States v. Microsoft Corp.*, 138 S.Ct. 1186, 584 U.S. __ (2018).

[111] Letter from Apple et al. to Senator Orrin Hatch et al., U.S. Senate (Feb. 6, 2018), *available at* https://www.scribd.com/document/374641879/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618#download&from_embed.

[112] *See, e.g.*, Neema S. Guliani & Naureen Shah, *The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them*, Lawfare (Mar. 16, 2018), https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them.

[113] Pub. L. 115-118, § 101(a).

[114] *Id.*

[115] *Id.* § 103.

[116] S. 3655, 115th Cong. (2018), *available at* https://www.congress.gov/bill/115th-congress/senate-bill/3655/text.

[117] S. 3655 § 3.

[118] *Id.* § 2(a)(1).

[119] *Id.*

[120] *Id.* § 5.

[121] Joseph Marks, *The Cybersecurity 202: Republicans and Democrats are feuding over the Equifax breach*, Washington Post (Dec. 11, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/12/11/the-cybersecurity-202-republicans-and-democrats-are-feuding-over-the-equifax-breach/5c0e9ec91b326b67caba2b5c/?utm_term=.092af4a07bd9.

[122] Dem. Staff of H. Comm. on Oversight and Gov't Reform and Comm. on Sci., Space and Tech., 115th Cong., *What the Next Congress Should Do to Prevent a Recurrence of the Equifax Data Breach* 3-7 (2018), *available at* https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/Equifax%20Minority%20Report%20-%20FINAL%2012-10-2018.pdf.

[123] Maj. Staff of H. Comm. on Oversight and Gov't Reform, 115th Cong., *The Equifax Data Breach* 94-96 (2018), *available at*https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf; *see also* Joseph Marks, *The Cybersecurity 202: Republicans and Democrats are feuding over the Equifax breach*, Washington Post (Dec. 11, 2018), *available at* https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/12/11/the-cybersecurity-202-republicans-and-democrats-are-feuding-over-the-equifax-breach/5c0e9ec91b326b67caba2b5c/?utm_term=.a267f7aa93c9.

[124] S. 2124, 115th Cong. (2018), *available at* https://www.congress.gov/bill/115th-congress/senate-bill/2124.

[125] 18 U.S.C. § 2703.

[126] *See* David Ruiz, *Email Privacy Act Comes Back, Hopefully to Stay*, *Electronic Frontier Found.* (May 29, 2018), https://www.eff.org/deeplinks/2018/05/email-privacy-act-comes-back-hopefully-stay; Letter from ACT: The App Association et al. to John McCain et al., U.S. Senate (July 13, 2018), https://cdt.org/files/2018/07/Email-Privacy-NDAA-sign-on-letter-final.pdf.

[127] *See* H.R. Rep. No. 115-874, at 965 (2018).

[128] National Conference of State Legislatures, *2018 Security Breach Legislation* (Oct. 12, 2018), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx.

[129] S.B. 318 (Ala. 2018), *available at* https://legiscan.com/AL/bill/SB318/2018.

[130] S.B. 62, 93rd Legis. Sess. (S.D. 2018), *available at* https://legiscan.com/SD/bill/SB62/2018.

[131] S.B. 361 (La. 2018), *available at* https://legiscan.com/LA/rollcall/SB361/id/75044; *see also* National Conference of State Legislatures, *2018 Security Breach Legislation* (Oct. 12, 2018), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx.

[132] Cal. Civ. Code § 1798.100.

[133] Rita Heimes and Sam Pfeifle, *New California privacy law to affect more than half a million US companies*, Int'l Ass'n of Privacy Prof'ls., (July 2, 2018), *available at* https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/.

[134] *See e.g.*, Letter from California Chamber of Commerce et al. to Senator Bill Dodd (Aug. 6, 2018), *available at* http://netchoice.org/wp-content/uploads/SB-1121-Final-Author-Coalition-Letter-2.8.7.2018.pdf.

[135] *Id.*

[136] Cal. Civ. Code § 1798.100, *et seq*.

[137] Cal. Civ. Code § 1798.150(a)(1).

[138] S.B. 1121 (Cal. 2018).

[139] Cal. Civ. Code § 1798.91.04.

[140] Cal. Civ. Code § 1798.91.04(a).

[141] Cal. Civ. Code § 1798.91.04(b).

[142] National Conference of State Legislatures, *2018 Security Breach Legislation* (Oct. 12, 2018), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx.

[143] S.B. 220, 132nd Leg. Sess. (Ohio 2018), https://legiscan.com/OH/text/SB220/id/1811629.

[144] *Id.*

[145] Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[146] Facebook, Inc.'s Motion to Dismiss Plaintiffs' Consolidated Shareholder Derivative Complaint, *In re Facebook, Inc. Shareholder Derivative Privacy Litigation*, No. 18-CV-01792 (N.D. Cal. Aug. 10, 2018), ECF Nos. 69-71.

[147] *See* Plaintiffs' Opposition to Motion of Defendant Facebook, Inc. to Dismiss Plaintiffs' Consolidated Complaint, *In re: Facebook, Inc. Consumer Privacy User Profile Litigation*, No. 18-MD-02843 (N.D. Cal. Nov. 30, 2018), ECF No. 208; Reply in Support of Motion of Defendant Facebook, Inc. to Dismiss Plaintiffs' Consolidated Complaint, *In re: Facebook, Inc. Consumer Privacy User Profile Litigation*, No. 18-MD-02843 (N.D. Cal. Dec. 21, 2018), ECF Nos. 233-34.

[148] David Thacker, *Expediting Changes to Google+*, Google (Dec. 10, 2018), https://www.blog.google/technology/safety-security/expediting-changes-google-plus/; Douglas MacMillan & Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, Wall Street Journal (Oct. 8, 2018), https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194.

[149] Lily Hay Newman, *A New Google+ Blunder Exposed Data from 52.5 Million Users*, Wired (Dec. 10, 2018), https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/.

[150] Complaint, *Matic v. Google*, No. 18-cv-06164 (N.D. Cal. Oct. 8, 2018), ECF No. 1.

[151] Complaint, *Mawardy v. Google*, No. 18-cv-05704 (E.D.N.Y. Oct. 11, 2018), ECF No. 1; Complaint, *Wicks v. Google*, No. 18-cv-06245 (N.D. Cal. Oct. 11, 2018), ECF No. 1; Rhode Island, *Rhode Island Suing Google Over Data Breach*, Rhode Island, https://www.ri.gov/press/view/34829.

[152] Nicholas Fandos & Michael Wines, *Russia Tried to Undermine Confidence in Voting Systems, Senators Say*, N.Y. Times (May 8, 2018), https://www.nytimes.com/2018/05/08/us/politics/russia-2016-election-hackers.html.

[153] *Id.*

[154] The United States Department of Justice Office of Public Affairs, *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election*, Department of Justice (July 13, 2018), https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

[155] Complaint, *Democratic National Committee v. The Russian Federation*, No. 18-cv-03501 (S.D.N.Y. Apr. 20, 2018), ECF No. 1.

[156] Memorandum of Law in Support of Defendant WikiLeaks's Pre-Trial Motion to Dismiss the First Amended Complaint, *Democratic National Committee v. the Russian Federation*, No. 18-CV-3501 (S.D.N.Y. Dec. 7, 2018) ECF No. 206.

[157] Marriott International, *Marriott Provides Update on Starwood Database Security Incident*, Marriott International (Jan. 4, 2019), http://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/.

[158] *See, e.g.*, Complaint, *Vetter v. Marriott Int'l, Inc.*, No. 19-cv-00094-RWT (D. Md. Jan. 9, 2019), ECF No. 1; *Fox v. Marriott Int'l, Inc.*, No. 18-07936 (N.D. Ill. Dec. 1, 2018), ECF No. 1; Complaint, *Perkins v. Marriott Int'l, Inc.*, No. 18-cv-12477 (D. Mass. Nov. 30, 2018), ECF No. 1.

[159] Complaint, *McGrath v. Marriott Int'l, Inc.*, 18-cv-06845 (E.D.N.Y. Dec. 1, 2018), ECF No. 1.

[160] Hamza Shaban, *Under Armour announces data breach, affecting 150 million MyFitnessPal app accounts*, Washington Post (Mar. 29, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/under-armour-announces-data-breach-affecting-150-million-myfitnesspal-app-accounts.

[161] MyFitnessPal, *MyFitnessPal Account Security Issue: Frequently Asked Questions*, https://content.myfitnesspal.com/security-information/FAQ.html.

[162] Motion to Compel Arbitration and to Dismiss or Stay Litigation, *Murray v. Under Armour, Inc.*, 18-cv-04032 (C.D. Cal. May 29, 2018), ECF No. 12.

[163] *Hudson's Bay Co. Customer Data Sec. Breach Litig.*, 326 F. Supp. 3d 1372 (U.S. Jud. Pan. Mult. Lit. 2018); *See also* Robert McMillan & Suzanne Kapner, *Saks, Lord & Taylor Hit With Data Breach*, Wall Street Journal (Apr. 2, 2018), https://www.wsj.com/articles/saks-lord-taylor-hit-with-data-breach-1522598460.

[164] *Id.*

[165] *Id.*

[166] *See* Class Action Complaint, *Joseph v. Saks Inc.*, No. 18-cv-04563 (S.D.N.Y. May 23, 2018), ECF No. 1; Class Action Complaint, *Rudolph v. Saks & Co. LLC*, No. 18-cv-05107 (C.D. Cal. June 8, 2018), ECF No. 1; Class Action, *Beekman v. Lord & Taylor, LLC*, No. 18-cv-00521 (D. Del. Apr. 5, 2018), ECF No. 1; Complaint—Class Action, *Sacklow v. Saks Inc.*, No. 3:18-cv-00360 (M.D. Tenn. Apr. 11, 2018), ECF No. 1.

[167] Order Denying Transfer, *In re: Hudson's Bay Co. Customer Sec. Data Breach Litig.*, MDL No. 2847 (U.S. Jud. Pan. Mult. Lit. Aug. 1, 2018), ECF No. 50.

[168] Sears Holdings Corporation Staff, Statement on Data Security Incident, Sears Holdings (Apr. 4, 2018), https://blog.searsholdings.com/shc-updates/statement-on-data-security-incident/.

[169] Delta Airlines, Inc, *Information on [24]7.AI Cyber Incident*, Delta (Apr. 7, 2018), https://www.delta.com/content/www/en_US/response.html.

[170] Complaint, *Naini v. Delta Air Lines, Inc.*, No. 18-cv-02876 (C.D. Cal. Apr. 6, 2018) ECF No. 1.

[171] Sean Keane, *Macy's Breach Exposed Customer Data, Credit Card Numbers*, CNET (July 11, 2018), https://www.cnet.com/news/macys-data-breach-may-have-seen-customer-info-stolen/; Complaint, *Carroll v. Macy's Inc.*, No. 18-cv-01060 (N.D. Ala. July 9, 2018), ECF No. 1.

[172] Thomas H. McCoy Jr., M.D., *Temporal Trends and Characteristics of Reportable Health Data Breaches*, 2010-2017, 320, Journal of the American Medical Association 1282 (2018).

[173] Unity Point Health, *Notice Regarding Security Incident*, UnityPoint Health, https://www.unitypoint.org/filesimages/About/Security%20Substitute%20Notification.pdf.

[174] *Id.*

[175] *Id.*

[176] Beth Jones Sanborn, *UnityPoint Health System Hit With Cyberattack Affecting 16,000 Patients*, Healthcare IT News (Apr. 20, 2018), https://www.healthcareitnews.com/news/unitypoint-health-system-hit-cyberattack-affecting-16000-patients.

[177] *Id.*

[178] Defendant's Memorandum of Law in Support of Its Motion to Dismiss Plaintiffs' Second Amended Complaint, *Fox v. Iowa Health System d/b/a UnityPoint Health*, No. 18-cv-00327 (W.D. Wis. Jun. 29, 2018), ECF No. 8.

[179] Beth Jones Sanborn, *LifeBridge Health Reveals Breach That Compromised Health Data of 500,000 Patients*, Health IT News (May 23, 2018), https://www.healthcareitnews.com/news/lifebridge-health-reveals-breach-compromised-health-data-500000-patients; DDS Issues Notice of Potential Breach of Confidential Information, State of California Department of Developmental Services, https://www.dds.ca.gov/SecurityNotice/.

[180] *See, e.g.*, Complaint, *Allen et al v. Equifax, Inc.*, No. 1:17-cv-04544 (N.D. Ga. Nov. 10, 2017), ECF No. 1; *see also* Wolf Richter, *Equifax's Data Breach Will Cost It for Months to Come*, Business Insider (Nov. 11, 2017), http://www.businessinsider.com/equifax-data-breach-will-keep-costing-it-for-months-to-come-2017-11.

[181] *See In re: Equifax, Inc. Customer Data Security Breach Litigation*, No. 17-md-2800 (N.D. Ga.).

[182] Memorandum in Support of Defendants' Motion to Dismiss the Financial Institutions' Consolidated Amended Complaint, *In re: Equifax, Inc. Customer Data Security Breach Litigation*, No. 17-md-2800 (N.D. Ga. July 16, 2018), ECF No. 435.

[183] Memorandum of Law in Support of Motion to Dismiss Consolidated Small Business Class Action Complaint, *In re: Equifax, Inc. Customer Data Security Breach Litigation*, No. 17-md-2800 (N.D. Ga. Aug. 8, 2018), ECF No. 441.

[184] Motion Hearing Held on 12/14/2018, *In re: Equifax, Inc. Customer Data Security Breach Litigation*, No. 17-md-2800 (N.D. Ga. Dec. 14, 2018) , ECF No. 534.

[185] *See, e.g.*, Complaint, *Bellwether Comm. Credit Union v. Chipotle Mexican Grill, Inc.*, No. 1:17-cv-01102 (D. Colo., May 4, 2017), ECF No. 1.

[186] Order, *Bellwether Community Credit Union v. Chipotle Mexican Grill, Inc.*, No. 17-cv-1102 (D. Colo. Oct. 24, 2018), ECF No. 83.

[187] *Id.*

[188] *In re: U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 266 F. Supp. 3d 1 (D.D.C. 2017).

[189] Brief for Appellants National Treasury Employees Union, *In re: U.S. Office of Personnel Management Data Security Breach Litigation*, No. 17-5217 (D.C. Cir. May 10, 2018), ECF No. 83; Brief of Amici Curiae Electronic Privacy Information Center (EPIC), *In re: U.S. Office of Personnel Management Data Security Breach Litigation*, No. 17-5217 (D.C. Cir. May 17, 2018), ECF No. 42.

[190] *Id.*

[191] Louis C. LaBrecque, *Unions, Federal Agency Set for Court Clash in Data Breach Case*, Bloomberg Law (Nov. 2, 2018), https://news.bloomberglaw.com/daily-labor-report/unions-federal-agency-set-for-court-clash-in-data-breach-case.

[192] *Attias v. CareFirst Inc.*, 865 F.3d 620, 622 (D.C. Cir. 2017).

[193] *Id.* at 623.

[194] *CareFirst, Inc. v. Attias*, 138 S. Ct. 981 (2018).

[195] Petition for a Writ of Certiorari, *CareFirst, Inc. v. Attias*, No. 17-641 (U.S. Oct. 30, 2017).

[196] *In re Zappos.com, Inc.*, 888 F.3d 1020, 1022 (9th Cir. 2018).

[197] *Id.*

[198] Petition for a Writ of Certiorari, *Zappos.com, Inc. v. Stevens*, No. 18-225 (U.S. Aug. 20, 2018).

[199] *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 829 (7th Cir. 2018).

[200] *Id.* at 828.

[201] *Id.* at 830.

[202] 136 S. Ct. 1540 (2016).

[203] *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017).

[204] *CareFirst, Inc. v. Attias*, 138 S. Ct. 981 (2018); Petition for a Writ of Certiorari, *CareFirst, Inc. v. Attias*, 865 F.3d 620 (D.C. Cir. Aug. 15, 2017).

[205] *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018).

[206] *Id.*

[207] Petition for a Writ of Certiorari, *Zappos.com, Inc. v. Stevens*, No. 18-225 (U.S. Aug. 20, 2018).

[208] *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89 (2d Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir.), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307 (2017); *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017).

[209] *See* Complaint, *In re The Wendy's Co. Shareholder Derivative Action*, No. 1:16-cv-01153 (S.D. Ohio Dec. 16, 2016), ECF No. 1; Memorandum of Law in Support of Plaintiff Thomas Caracci's Motion for a Status Conference, *In re The Wendy's Co. Shareholder Derivative Action*, No. 1:16-cv-01153 (S.D. Ohio Dec. 6, 2018), ECF No. 48. A consumer class action lawsuit against Wendy's arising of the same data breach also settled. *See Torres v. Wendy's International, LLC*, No. 6:16-cv-00210 (M.D. Fla.).

[210] Plaintiff James Graham's Motion for Preliminary Approval of Derivative Litigation Settlement, *In re The Wendy's Co. Shareholder Derivative Action*, No. 1:16-cv-01153, 2018 WL 2328335 (S.D. Ohio May 6, 2018), ECF No. 41.

[211] *Id.*

[212] *Id.*

[213] Class Action Complaint, *Wicks v. Alphabet, Inc.*, No. 4:18-cv-06245, 2018 WL 4941767 (C.D. Cal. Oct. 11, 2018), ECF No. 1.

[214] *Id.*

[215] Order Granting Stipulation, *Wicks v. Alphabet, Inc.*, No. 4:18-cv-06245 (N.D. Cal. Nov. 7, 2018), ECF No. 14.

[216] Class Act[ion] Complaint, *Shah v. Chegg, Inc.*, No. 3:18-cv-05956 (N.D. Cal. Sept. 27, 2018), ECF No. 1.

[217] *Id.*

[218] *See* Order, *Shah v. Chegg, Inc.*, No. 3:18-cv-06714 (N.D. Cal. Dec. 12, 2018), ECF No. 10; Class Action Complaint, *Kurland v. Chegg, Inc.*, No. 3:18-cv-06714, 2018 WL 5835331 (N.D. Cal. Nov. 5, 2018), ECF No. 1.

[219] *See In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 967 (N.D. Cal. 2016).

[220] *See generally* Order Granting Motion for Preliminary Approval of Class Action Settlement, *In re Anthem*, No. 5:15-md-02617-LHK, (N.D. Cal. Aug. 25, 2017), ECF No. 903.

[221] *See* Order, *In re Anthem*, No. 5:15-md-02617-LHK, (N.D. Cal. Aug. 15, 2018), ECF No. 1046.

[222] *Id.*

[223] Letter to Customers: T-Mobile's CEO on Experian's Data Breach, *https://www.t-mobile.com/customers/experian-data-breach*.

[224] *Id.*

[225] Class Action Settlement Agreement and Release, *In re Experian Data Breach Litigation*, No. 15-CV-01592 (C.D. Cal., Nov. 12, 2018), ECF No. 285.

[226] *Id.*

[227] *Id.*

[228] *See* Brief for Petitioners, *Frank v. Gaos*, No. 17-961 (U.S. July 9, 2018).

[229] Jimmy Hoover, *Google Settlement Snubbed Class Members, Justices Told*, Law360 (Oct. 31, 2018), https://www.law360.com/articles/1097634/google-settlement-snubbed-class-members-justices-told.

[230] Brief for Petitioners, *Frank v. Gaos*, No. 17-961 (U.S. July 9, 2018).

[231] Ronald Mann, *Argument Analysis: Justices Skeptical of "Cy Pres" Class-Action Settlements*, SCOTUSBlog (Nov. 1, 2018) http://www.scotusblog.com/2018/11/argument-analysis-justices-skeptical-of-cy-pres-class-action-settlements/.

[232] *Id.*

[233] Order, *Frank v. Gaos*, No. 17-961 (U.S. Nov. 6, 2018).

[234] *See* Order, *In re Anthem*, No. 5:15-md-02617-LHK, (N.D. Cal. Aug. 15, 2018), ECF No. 1046.

[235] *See* Final Order and Judgment at 3–6, *In re Home Depot*, No. 1:14-md-02583-TWT (N.D. Ga. Sept. 22, 2017), ECF No. 343.

[236] Order Granting Final Approval of Class Action Settlement and Final Judgment, *In re Home Depot*, No. 1:14-md-02583-TWT (N.D. Ga. Aug. 23, 2016), ECF No. 260 (adopting Settlement

Agreement, ECF No. 181-2); Order Granting Consumer Plaintiffs' Motion For Service Awards, Attorneys' Fees and Litigation Expense Reimbursement, No. 1:14-md-02583-TWT (N.D. Ga. Aug. 23, 2016), ECF No. 261 (adopting Settlement Agreement, ECF No. 181-2).

[237] Mem. and Order Granting Mot. for Final Approval of Financial Institutions' Class Action Settlement and Mot. for Att'y Fees and Expenses and Service Payments, *In re Target*, No. 0:14-md-02522-PAM (D. Minn. May 12, 2016), ECF No. 758 (adopting Settlement Agreement, ECF No. 653-1).

[238] Robin Sidel, *Target to Settle Claims Over Data Breach*, Wall St. J. (Aug. 18, 2015, 5:10 PM ET), http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013.

[239] Final Approval of Class Settlement, *In re Sony*, No. 2:14-cv-09600-RGK-E (C.D. Cal. Apr. 6, 2016), ECF No. 165 (approving Settlement Agreement, ECF No. 146-1); Order on Mot. for Att'y Fees, Costs, and Service Awards at 3, *In re Sony*, No. 2:14-cv-09600-RGK-E (C.D. Cal. Apr. 12, 2016), ECF No. 166.

[240] *St. Joseph Health System Med. Info. Cases*, JCCP No. 4716 (Cal. Sup. Ct.). Gibson Dunn represented St. Joseph in this case.

[241] Mem. and Order Granting Mot. for Final Approval of Consumer Settlement and Mot for Payment of Service Awards and Fees and Expenses, *In re Target*, No. 0:14-md-02522-PAM (D. Minn. Nov. 16, 2016), ECF No. 645 (approving Settlement Agreement, ECF No. 358-1).

[242] Order Granting Final Approval of Class Action Settlement, *In re LinkedIn User Privacy Litig.*, No. 12-CV-03088-EJD (N.D. Cal. Sept. 15, 2015), ECF No. 147 (approving Settlement Agreement, ECF No. 145-1).

[243] Mot. for Approval of Voluntary Dismissal, *In re Adobe Systems Inc. Privacy Litig.*, No. 5:13-CV-05226-LHK (N.D. Cal. June 9, 2015), ECF No. 87; Settlement Agreement, *In re Adobe Systems Inc. Privacy Litig.*, No. 5:13-CV-05226-LHK (N.D. Cal. June 9, 2015), ECF No. 87-2.

[244] Min. Order Granting Motion for Settlement, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. 3:11-md-02258 (S.D. Cal. May 4, 2015), ECF No. 210; Settlement Agreement, *In re Sony Gaming Networks*, No. 3:11-md-02258 (S.D. Cal. June 13, 2014), ECF No. 190-2.

[245] *Cooper v. Slice Techs., Inc.*, No. 17-CV-7102 (JPO), 2018 WL 2727888, at *5 (S.D.N.Y. June 6, 2018).

[246] *Id.*

[247] *Id.*

[248] *Id.* at *4.

[249] *Id.* (quoting the agreement language in the plaintiffs' complaint).

[250] 18 U.S.C. § 2511(2)(d).

[251] Cal. Penal Code § 630, *et seq*.

[252] *See Bona Fide Conglomerate, Inc. v. SourceAmerica*, No. 3:14-CV-00751-GPC, 2016 WL 3543699, at *6 (S.D. Cal. June 29, 2016) (citing *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022, 1028 (N.D. Cal. 2011)); *see also Carrese v. Yes Online Inc.*, No. 16-CV-05301-SJO, 2016 WL 6069198, at *4 (C.D. Cal. Oct. 13, 2016).

[253] *Mulder v. Wells Fargo Bank, N.A.*, No. 2:18-CV-00029, 2018 WL 3750627, at *7 (W.D. Pa. July 10, 2018).

[254] *Id.* at *1.

[255] *Id*. at *4-5.

[256] *Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427 (Ct. App. 2018)

[257] *Id.* at 430.

[258] *Id.*

[259] *Id.* at 433-34.

[260] *Id.* at 435 (quoting *People v. Superior Court of Los Angeles Cty.*, 70 Cal. 2d 123, 134 (1969)) (alterations omitted).

[261] *Id.*

[262] Plaintiff's Motion for Preliminary Approval of Proposed Class Action Settlement (Unopposed), *In re Vizio, Inc., Consumer Privacy Litig.*, No. 8:16-ml-02693-JLS-KES (C.D. Cal. Oct. 4, 2018), ECF No. 282-2.

[263] Complaint, *In re Vizio, Inc., Consumer Privacy Litig.*, No. 8:16-ml-02693-JLS-KES (C.D. Cal. Mar. 23, 2017), ECF No. 1.

[264] *Id*.

[265] Second Consolidated Amended Complaint, *In re Vizio, Inc., Consumer Privacy Litig.*, No. 8:16-ml-02693-JLS-KES (C.D. Cal. Mar. 23, 2017), ECF No. 136.

[266] Plaintiff's Motion for Preliminary Approval of Proposed Class Action Settlement (Unopposed), *In re Vizio, Inc.*, Consumer Privacy Litig., No. 8:16-ml-02693-JLS-KES (C.D. Cal. Oct. 4, 2018), ECF No. 282-2.

[267] *Cohen v. Casper Sleep Inc.*, No. 17CV9325, 2018 WL 3392877, at *1 (S.D.N.Y. July 12, 2018).

[268] *Id.*

[269] *Id.* at *3.

[270] *Id.* at *4.

[271] *Id*. at *5 (quoting *Ashcroft v. Iqbal*, 556 U.S. 678 (2009)).

[272] *Allen v. Quicken Loans Inc*., No. CV1712352ESMAH, 2018 WL 5874088, at *2 (D.N.J. Nov. 9, 2018).

[273] *Id.* at *4 (internal quotation marks omitted).

[274] *Id.* at *12.

[275] 47 U.S.C. §§ 227 *et seq.*

[276] 885 F.3d 687 (D.C. Cir. 2018). Gibson Dunn represented the U.S. Chamber of Commerce, one of the petitioners, in this case.

[277] *Id.* at 695.

[278] 47 U.S.C § 227(a)(1).

[279] *Id*. at 696-97.

[280] *Id*. at 697.

[281] 47 U.S.C § 227(a)(1).

[282] *ACA International*, 885 F.3d at 701.

[283] *Id*. at 702.

[284] *Id*. at 703.

[285] 894 F.3d 116, 120-21 (3d Cir. 2018).

[286] *Id*. at 121.

[287] *Id*.

[288] 904 F.3d 1041 (9th Cir. 2018).

[289] *Id*. at 1051-53.

[290] *Id*.

[291] *Id.* at 1052.

[292] Federal Communications Commission, *Consumer And Governmental Affairs Bureau Seeks Comment On Interpretation Of The Telephone Consumer Protection Act In Light Of The D.C. Circuit's ACA International Decision* (May 14, 2018), *available at*https://ecfsapi.fcc.gov/file/0514497027768/DA-18-493A1.pdf.

[293] Federal Communications Commission, *Consumer And Governmental Affairs Bureau Seeks Further Comment On Interpretation Of The Telephone Consumer Protection Act In Light Of The Ninth Circuit's Marks v. Crunch San Diego, LLC Decision* (Oct. 3, 2018), *available at*https://ecfsapi.fcc.gov/file/0514497027768/DA-18-493A1.pdf.

[294] No. 17-1705, 2018 WL 3127423 (2018).

[295] *Id.*

[296] *See Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 843 (1984)

[297] *Carlton & Harris Chiropractic v. PDR* Network, 882 F.3d 459, 464 (4th Cir. 2018).

[298] *Id.*

[299] No. 17-1705, 2018 WL 3127423 (U.S. Nov. 13, 2018).

[300] Griffin Connolly, *Lawmakers Want to Curb Those Pesky Robocalls to Your Phone*, Roll Call (Jun. 11, 2018), *available at*https://www.rollcall.com/news/policy/lawmakers-want-curb-pesky-robocalls-phone.

[301] *Id.*

[302] United States Senate Committee on Commerce, Science, & Transportation, Press Release, *Bipartisan TRACED Act Cracks Down on Illegal Robocall Scams* (Nov. 16, 2018), *available at* https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=91889B92-62FE-4AF1-A6A4-D26E7E2F296F.

[303] *White v. Samsung Electronics America, Inc., et al.*, No. 17-1775 (D.N.J. Sept. 26, 2018).

[304] *Id.* at *4-5.

[305] 18 U.S.C. § 2710(a)(3).

[306] Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, New York Times (Mar. 13, 2018), *available at*https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.

[307] Sopan Deb and Natasha Singer, *Taylor Swift Said to Use Facial Recognition to Identify Stalkers*, New York Times (Dec. 13, 2018), *available at*https://www.nytimes.com/2018/12/13/arts/music/taylor-swift-facial-recognition.html.

[308] Mastercard Biometric Card FAQs, Mastercard.com, *available at* https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html.

[309] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(o)(1)(E).

[310] 740 Ill. Comp. Stat. Ann. 14/20.

[311] 2018 WL 4699213 (Ill. App 1st Sept. 28, 2018).

[312] *Id*. at *1.

[313] 2017 WL 6523910 (IL App 2nd Dec. 21, 2017). *Rosenbach v. Six Flags Entertainment Corp.* is discussed in further detail in last year's Year-End Update: https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2018/.

[314] 2018 WL 4699213, at *1.

[315] 2018 WL 2445292 (N.D. Ill. May 31, 2018).

[316] 2018 WL 4699213, at *1.

[317] *Rosenbach v. Six Flags Entm't Corp.*, No. 123186 ¶ 1 (Ill. Jan. 25, 2019).

[318] *Id.* ¶ 34.

[319] *Id.* ¶ 37.

[320] S.B. 3053, 2018 Reg. Sess. (Ill. 2018).

[321] Peter Newman, *The Internet of Things 2018 Report: How the IoT is Evolving to Reach the Mainstream with Businesses and Consumers*, BUS. INSIDER INTELLIGENCE (Feb. 26, 2018), *available at* http://www.businessinsider.com/the-internet-of-things-2017-report-2018-2-26-1.

[322] Senate Bill No. 327, Assembly Bill No. 1906, California 2017-2018 Regular Session (codified at 1.81.26 of Part 4 of Division 3 of California Civil Code); *see* Gibson Dunn Client Alert: New California Security of Connected Devices Law and CCPA Amendments (Oct. 5, 2018), *available at*https://www.gibsondunn.com/new-california-security-of-connected-devices-law-and-ccpa-amendments/.

[323] *Id.* at § 1798.91.04(a), 1798.91.05(b).

[324] *Id.* at § 1798.91.04(b).

[325] *Id.* at § 1798.91.06(a)-(b).

[326] *Id.* at § 1798.91.06(e).

[327] *See* Theo Douglas, *California Governor Approves Bills Tightening Security, Privacy of IoT Devices*, Govtech.com (Sept. 28, 2018), *available at*http://www.govtech.com/applications/Two-Bills-Before-California-Governor-Would-Tighten-Security-Privacy-of-IoT-Devices.html. The CMTA explained that because the bill only applies to California manufacturers, it creates a "loophole" for imported devices to avoid the security feature requirements, thereby making the state less attractive for manufacturers.

[328] *Id.*

[329] Robert Graham, *California's bad IoT law*, Errata Security blog (Sept. 10, 2018), *available at* https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XCY-9cL2bmi.

[330] Derek Hawkins, Derek, *The Cybersecurity 202: California's Internet of Things cybersecurity bill could lay groundwork for federal* action, The Washington Post (Sept. 17, 2018).

[331] H.R. 6032, 115th Cong. (2018).

[332] Fact Sheet, Internet of Things Cybersecurity Improvement Act of 2017, *available at* https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act—fact-sheet.pdf.

[333] H.R. 1234, 115th Cong. (2018).

[334] S. 88 and H.R. 686, 11th Cong. (2017). The Act was passed by the Senate in August 2017 but has not yet passed the House.

[335] H.R. 4163 and S. 2020, 115th Cong. (2017).

[336] S. 2234, 115th Cong. (2017).

[337] Notice by Consumer Product Safety Commission, 83 FR 13122, *available at* https://www.federalregister.gov/documents/2018/03/27/2018-06067/the-internet-of-things-and-consumer-product-hazards.

[338] Public Hearing on the Internet of Things and Consumer Product Hazards, U.S. Consumer Product Safety Commission (May 16, 2018), *available at* https://cpsc.gov/s3fs-public/Panelists%20Presentations%20-

%20IoT%20and%20Consumer%20Product%20Hazards%20%20Public%20Hearing%20-%20May%2016%202018.pdf?q3A.aOH4qiLleXB3TybNrHi9mwt4yM77.

[339] Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection, *In the Matter of The Internet of Things and Consumer Product Hazards*, Docket No. CPSC-2018-007 (June 15, 2018), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf.

[340] *Id.* at 6-8.

[341] *Id.* at 4, 11.

[342] Prepared Remarks of Commissioner Rebecca Kelly Slaughter, *Visions and Goals for the Future of IoT in the USA and Globally*, Federal Trade Commission (Oct. 4, 2018), *available at* https://www.ftc.gov/system/files/documents/public_statements/1414540/20181004_prepared_remarks_of_commissioner_slaughter_for_the_forum_global_6th_annual_iot_global.pdf

[343] *Id.* at 2.

[344] *Id.* at 3-4.

[345] *Id.* at 5-6.

[346] Order Granting in part and Denying in part Defs.' Mot. for Summ. Judgment at 1, *Flynn v. FCA US LLC*, No. 15-cv-00855-MJR-DGW (July 5, 2018), ECF No. 399; Compl., *Flynn v. FCA US LLC*, No. 15-cv-00855-MJR-DGW, 2017 WL 3592040, (S.D. Ill. Dec. 22, 2015).

[347] Order Granting in part and Denying in part Defs.' Mot. for Summ. Judgment at 1, *Flynn v. FCA US LLC*, No. 15-cv-00855-MJR-DGW (July 5, 2018), ECF No. 399. As discussed in last year's Review, in August 2017, the court dismissed all of the plaintiffs' claims that possible future car hacking could cause injury or death but allowed plaintiffs to pursue claims that they overpaid for the vehicles in light of the alleged system vulnerabilities. *Flynn v. FCA US LLC*, No. 15-cv-00855-MJR-DGW, 2017 WL 3592040, at *5 (S.D. Ill. Aug. 21, 2017).

[348] Order at 1, *Flynn v. FCA US LLC*, No. 15-cv-00855-MJR-DGW, 2017 WL 3592040, at *5 (Nov. 29, 2018), ECF No. 448.

[349] Plaintiffs' Notice of Motion and Motion for Preliminary Approval of Proposed Class Action Settlement (Unopposed), *In Re: Vizio, Inc., Consumer Privacy Litigation*, 8:16-ml-02693 (C.D. Cal. Oct. 4, 2018), ECF No. 282.

[350] *Id.*

[351] Order Granting Plaintiffs' Motion for Preliminary Approval of Class Action Settlement, *In Re: Vizio, Inc., Consumer Privacy Litigation*, 8:16-ml-02693 (C.D. Cal. Jan. 4, 2019), ECF No. 297.

[352] *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, Federal Trade Commission (Feb. 6, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[353] 18 U.S.C. § 1030.

[354] *See EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577, 581-82 (1st Cir. 2001); *United States v. John*, 597 F.3d 263, 272-73 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258, 1263-64 (11th Cir. 2010).

[355] *See United States v. Valle*, 807 F.3d 508, 523-28 (2d Cir. 2015); *WEC Carolina Energy Sol.s LLC v. Miller*, 687 F.3d 199, 204-07 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854, 856-63 (9th Cir. 2012) (en banc).

[356] 291 F. Supp. 3d 659, 666 (E.D. Pa. 2018).

[357] *Id*. at 669.

[358] *Id*. at 670.

[359] No. 17 C 06318, 2018 WL 2933636 (N.D. Ill. June 12, 2018).

[360] *Id.* at *1-2.

[361] *Id*. at *3.

[362] *Id*.

[363] *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164 (C.D. Cal. 2018).

[364] *Id*. at 1175.

[365] *Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1171–72 (C.D. Cal. 2018).

[366] 315 F. Supp. 3d 1, 23 (D.D.C. 2018).

[367] *Cyber attack victims face disputes with insurers*, Financial Times (Dec. 2, 2018) https://www.ft.com/content/3679fd84-e9c2-11e8-a34c-663b3f553b35.

[368] Alicja Grzadkowska, *How cybercrime and coverage evolved in 2018*, Insurance Business America (Dec. 12, 2018),https://www.insurancebusinessmag.com/us/news/cyber/how-cybercrime-and-coverage-evolved-in-2018-118721.aspx.

[369] Justin Lynch, *Cyberattacks are increasing, and so is cyber insurance*, Fifth Domain (Dec. 10, 2018),https://www.fifthdomain.com/industry/2018/12/10/cyberattacks-are-increasing-and-so-is-cyber-insurance.

[370] *See* Scott Neil, *Marriott breach underlines cyber-risk scale*, Royal Gazette (Dec. 7, 2018), http://www.royalgazette.com/re-insurance/article/20181207/marriott-breach-underlines-cyber-risk-scale.

[371] *See* Erin Illman & Alex Purvis, *2 Recent Decisions May Affect your Cyber* Policy, Law360 (Nov. 2, 2018) https://www.law360.com/articles/1098216.

[372] *See* Scott Neil, *Marriot breach underlines cyber-risk scale*, Royal Gazette (Dec. 7, 2018), http://www.royalgazette.com/re-insurance/article/20181207/marriott-breach-underlines-cyber-risk-scale; Jeff Sistrunk, *Top Insurance Legislation & Regulation Stories of 2018*, Law360 (Dec. 13, 2018), https://www.law360.com/articles/1109766/top-insurance-legislation-regulation-stories-of-2018.

[373] *See e.g.*, *Sompo International Forms Cyber Team, Expands Insurance Offering*, Insurance Journal (Dec. 11, 2018), https://www.insurancejournal.com/news/national/2018/12/11/511645.htm; *AXA XL Adds Cybersecurity Services to Cyber Insurance Program*, Insurance Journal (Nov. 30, 2018), https://www.insurancejournal.com/news/national/2018/11/30/510695.htm.

[374] *See e.g.*, *Sompo International Forms Cyber Team, Expands Insurance Offering*, Insurance Journal (Dec. 11, 2018), https://www.insurancejournal.com/news/national/2018/12/11/511645.htm.

[375] *See e.g.*, *AXA XL Adds Cybersecurity Services to Cyber Insurance Program*, Insurance Journal (Nov. 30, 2018), https://www.insurancejournal.com/news/national/2018/11/30/510695.htm.

[376] *See* Alicja Grzadkowska, *How cybercrime and coverage evolved in 2018*, Insurance Business America (Dec. 12, 2018),https://www.insurancebusinessmag.com/us/news/cyber/how-cybercrime-and-coverage-evolved-in-2018-118721.aspx.

[377] *See* Terry Gangcuangco, *Cyber insurance hit with barrage of criticism as disputes mount*, Insurance Business UK (Dec. 3, 2018),https://www.insurancebusinessmag.com/uk/news/cyber/cyber-insurance-hit-with-barrage-of-criticism-as-disputes-mount-117720.aspx.

[378] *See* Justin Lynch, *Cyberattacks are increasing, and so is cyber insurance*, Fifth Domain (Dec. 10, 2018),https://www.fifthdomain.com/industry/2018/12/10/cyberattacks-are-increasing-and-so-is-cyber-insurance.

[379] *See Cyber attack victims face disputes with insurers*, Financial Times (Dec. 2, 2018) https://www.ft.com/content/3679fd84-e9c2-11e8-a34c-663b3f553b35.

[380] Jeff Sistrunk, *The Biggest Property & Casualty Insurance Decisions of 2018*, Law360 (Dec. 14, 2018), https://www.law360.com/articles/1102073/the-biggest-property-casualty-insurance-decisions-of-2018.

[381] *Medidata Sols. Inc., v. Fed. Ins. Co.*, 729 F. App'x 117, 119 (2d Cir. 2018).

[382] *Medidata Sols., Inc. v. Fed. Ins. Co.*, No. 15-CV-907 (ALC), 2017 WL 3268529, at *1–2 (S.D.N.Y. July 21, 2017).

[383] *Id.* at *5.

[384] *Medidata Sols. Inc.*, 729 F. App'x at 118.

[385] *Id.* (citing *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 25 N.Y.3d 675, 681 (2015)).

[386] *Id.*

[387] *Id.*

[388] *Id.* at 119.

[389] *American Tooling Ctr., Inc. v. Travelers Cas. and Sur. Co. of Am.*, No. 16-12108, 2017 WL 3263356 at *3 (E.D. Mich. Aug. 1, 2017).

[390] *American Tooling Ctr., Inc. v. Travelers Cas. and Sur. Co. of Am.*, 895 F.3d 455, 462 (6th Cir. 2018).

[391] *Id.* at 463.

[392] *St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.*, 2018 WL 4732718, at *1 (M.D. Fla. 2018).

[393] *Id.*

[394] *Id.* at *5.

[395] *Id.* at *6.

[396] *Innovak International, Inc. v. Hanover Insurance Company*, 280 F.Supp.3d 1340 (M.D. Fla. 2017).

[397] *Id.* at 1343.

[398] *St. Paul Fire*, 2018 WL 4732718, at *5 (quoting *Innovak International, Inc.* 280 F.Supp.3d at 1342, 1348) (internal alterations and citations omitted).

[399] *Id.*

[400] *St. Paul Fire & Marine Ins. v. Rosen Hotels & Resorts, Inc., et al.*, No. 18-14427-A (11th Cir. 2018).

[401] Complaint, *Nat'l Bank of Blacksburg vs. Everest Nat'l Insurance Co.*, No. 7:18-cv-00310-GEC (W.D. Va. Jun. 28, 2018).

[402] *Id.*

[403] *Id.*

[404] Answer, *Nat'l Bank of Blacksburg vs. Everest Nat'l Insurance Co.*, No. 7:18-cv-00310-GEC (W.D. Va. Jul. 20, 2018).

[405] 18 U.S.C. §§ 2510-22.

[406] U.S. Dep't of Justice, Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22 (July 30, 2017), https://it.ojp.gov/privacyliberty/authorities/statutes/1285.

[407] 18 U.S.C. § 2511.

[408] 18 U.S.C. § 2701-12.

[409] *Id.*

[410] *Id.*

[411] Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, §§ 101-106 (2018).

[412] H.R. 387, 115th Cong. (2017).

[413] H.R. 5515, 115th Cong. (2018).

[414] *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

[415] 18 U.S.C. § 2703.

[416] Letter from ACT: The App Association et al. to John McCain et al., U.S. Senate (July 13, 2018), https://cdt.org/files/2018/07/Email-Privacy-NDAA-sign-on-letter-final.pdf.

[417] H.R. Rep. No. 115-874, at 965 (2018).

[418] S. 1654, 115th Cong. (2017) (noting that the bill was twice referred to the Senate Judiciary Committee).

[419] *United States v. Microsoft Corp*., 138 S. Ct. 356 (2017)

[420] *United States v. Microsoft Corp.*, 138 S. Ct. 1186, 1187 (2018).

[421] Brief for Respondent at 20-37, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2).

[422] Brief for Petitioner at 21-25, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2).

[423] Oral Argument at 6, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2).

[424] 18 U.S.C. § 2713 (emphasis added).

[425] *Microsoft*, 138 S. Ct. at 1188 (explaining that "[n]o live dispute remains between the parties over the issue with respect to which certiorari was granted."); *see also* Gibson Dunn Client Alert: Supreme Court Holds That Recent Legislation Moots Dispute Over Emails Stored Overseas (April 17, 2018), *available at* https://www.gibsondunn.com/supreme-court-holds-that-recent-legislation-moots-dispute-over-emails-stored-overseas/.

[426] 18 U.S.C. § 2703(h)(2).

[427] 18 U.S.C. § 2523.

[428] 50 U.S.C. §§ 1801-1805.

[429] H. Permanent Select Comm. on Intelligence, *FISA Section 702*, https://intelligence.house.gov/fisa-702/.

[430] 50 U.S.C. § 1801(e).

[431] 50 U.S.C. § 103(a).

[432] James C. Duff, *Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017*, Administrative Office of the United States Courts (Apr. 25, 2018), http://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf.

[433] H. Permanent Select Comm. on Intelligence, *FISA Section 702*, *supra* note 429.

[434] *See, e.g.*, *United States v. Hasbajrami*, No. 11-CR-623 (JG), 2016 WL 1029500 at *16 (E.D.N.Y. Mar. 18, 2016) (denying defendant's constitutional challenge to Section 702 arguing that the

FBI was required to obtain a warrant before acquiring U.S. persons' communications incidentally gathered through lawful targeting of foreign persons).

[435] Pub. L. 115-118, § 103.

[436] *Id.* § 101(a).

[437] *Id.* § 203(a)(1).

[438] *See* Gibson Dunn Client Alert: Supreme Court Holds That Individuals Have Fourth Amendment Privacy Rights In Cell Phone Location Records (June 22, 2018), *available at* https://www.gibsondunn.com/supreme-court-holds-that-individuals-have-fourth-amendment-privacy-rights-in-cell-phone-location-records/.

[439] *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018).

[440] *Id.* at 2213.

[441] *Id.* at 2219; *see Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

[442] *Carpenter*, 138 S. Ct. at 2223.

[443] *Id.* at 2220, 2223.

[444] *Id.* at 2223.

[445] *Id.* at 2220 (citing *Riley v. California*, 124 S. Ct. 2473, 2484 (2014)).

[446] *Carpenter*, 138 S. Ct. at 2220.

[447] *Id.* at 2216.

[448] *See United States v. Jones*, 565 U.S. 400, 404 (2012); *Riley*, 124 S. Ct. at 2485.

[449] *Alasaad v. Nielsen*, No. 17-CV-11730-DJC, 2018 WL 2170323, at *20 (D. Mass. May 9, 2018).

[450] *Id.* at *14.

[451] *Riley*, 124 S. Ct. at 2485.

[452] *Alasaad*, 2018 WL 2170323, at *20.

[453] *United States v. Kolsuz*, 890 F.3d 133, 136-37 (4th Cir. 2018).

[454] *Id.* at 136.

[455] *Id.*

[456] *Id.* at 137.

[457] *Id.*

[458] *Id.*

The following Gibson Dunn lawyers prepared this client update: Alexander Southwell, Ryan Bergsieker, Eric Vandevelde, Howard Hogan, Josh Jessen, Lindsey Young, Jeremy Smith, Amy Chmielewski, Reid Rector, Cassandra Gaedt-Scheckter, Alexandra Perloff-Giles, Tony Bedel, Zoey Goldnick, Lucie Duvall, Josiah Clarke, Craig Streit, Jon Newmark, Sheri Pan, Jacob Rierson, and Luke Sullivan.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work or any of the following leaders and members of the firm's Privacy, Cybersecurity and Consumer Protection practice grou:

United States

Alexander H. Southwell – Co-Chair, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
M. Sean Royall – Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Christopher Chorba – Los Angeles (+1 213-229-7396, cchorba@gibsondunn.com)
Richard H. Cunningham – Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Shaalu Mehra – Palo Alto (+1 650-849-5282, smehra@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Europe

Ahmed Baladi – Co-Chair, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0)207071 4250, jacox@gibsondunn.com)

Patrick Doris – London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Penny Madden – London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen – London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)

Asia
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)