GIBSON DUNN

January 25, 2018

U.S. CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2018

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 sixth edition of Gibson Dunn's Cybersecurity and Data Privacy Outlook and Review. In 2017, companies were again challenged to navigate a constantly evolving landscape of cybersecurity and privacy issues. Last year revealed some of the largest data breaches in history, saw a new administration's shift in priorities regarding cybersecurity, and exposed new challenges posed by increasingly "smart" and connected devices.

Among other key regulatory developments this year, the Trump administration issued an executive order addressing the cybersecurity of federal networks and critical infrastructure. The Securities and Exchange Commission ("SEC") announced a new Cyber Unit focused on targeting cyber-related misconduct and pursued cases involving novel cyber issues, including insider trading in the wake of a data breach. The Federal Trade Commission ("FTC") remained active in the privacy and cybersecurity space, but indicated a shift of focus to cases involving "substantial consumer injury." The Department of Health and Human Services ("HHS") continued enforcement of regulations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), announcing several notable settlements. The Federal Communication Commission's ("FCC") role in privacy enforcement was substantially adjusted following the repeal of privacy rules put in place in 2016. And state attorneys general were active at the forefront of concerted efforts to bring enforcement actions and develop privacy and cybersecurity regulations. Indicative of this collaboration, 2017 saw the largest state data breach settlement in history.

Last year also saw frequent data breaches of varying magnitudes. Throughout the year, hackers targeted government agencies and companies in every industry, seeking personally identifiable information ("PII"), customer login information, payment information, and health care information, among others. As litigation—especially class action litigation—quickly followed many of the announced breaches, courts continued to grapple with standing issues in the wake of *Spokeo, Inc. v. Robins*. New class actions related to connected devices, such as TVs and cars, were also filed in 2017, and 2018 will likely see developments in this arena as more courts begin assessing standing in the context of the Internet of Things.

Overlapping international privacy frameworks also posed significant challenges for U.S. companies in 2017. With the quickly approaching May 2018 deadline for compliance with Europe's General Data Protection Regulation ("GDPR"), companies worked to put in place appropriate policies and other safeguards. Last year also saw many other countries impose new or updated cybersecurity and data privacy regulations.

We cover these topics and many more in this year's Review: (I) U.S. regulation of privacy and data security; (II) civil litigation; (III) international regulation of privacy and data security; and (IV) government data collection and device unlocking. For additional coverage of international developments, please see our separate International Cybersecurity and Data Privacy Outlook and Review.

Table of Contents

I. U.S. Regulation of Privacy and Data Security

Companies doing business in (and with) the United States continue to face a morass when it comes to government regulation of privacy and data security due to the competing and overlapping efforts of myriad federal and state government regulators in this space. Nearly every major federal agency has now weighed in on data security issues in one form or another, as have most states. Below, we cover the most notable enforcement efforts, regulatory guidance, and legislative developments from the past year.

A. Enforcement and Guidance

1. Federal Trade Commission ("FTC")

In 2017, the FTC remained one of the most active and far-reaching government agencies regulating privacy and data security. All told, the FTC announced 12 enforcement actions related to privacy and data security issues, while also making headlines with its related public statements and guidance. We address the most notable enforcement actions and guidance from the FTC below.

a. Data Security and Privacy Enforcement

Equifax . In September 2017, the FTC announced it had begun investigating the massive data breach at Equifax Inc., the Atlanta-based consumer credit bureau. [1] The week before the announcement, Equifax revealed that in May, hackers had exploited a flaw in the company's website that allowed them to access the account information of up to 143 million customers, including driver's license numbers, addresses, birthdates, and Social Security numbers. This breach represented one of the largest in recent memory and, given the centrality of credit-reporting agencies to activity throughout the economy and the sensitive nature of the information involved, sparked renewed public scrutiny of data security issues. The FTC did not elaborate on the scope of its investigation, but the announcement itself was significant given that the Commission rarely comments on ongoing investigations.

TaxSlayer . Further underscoring the FTC's increased attention to companies that store consumer financial data, in August 2017 the Georgia-based online tax preparation service TaxSlayer, LLC, agreed to settle FTC allegations that it allowed hackers to access nearly 9,000 user accounts between October and December 2015. [2] The hackers then used this information to fraudulently obtain tax returns. The FTC alleged that TaxSlayer failed to implement adequate security measures, such as requiring strong passwords, providing a clear and conspicuous privacy notice, or conducting risk assessments. As part of the settlement, TaxSlayer agreed to obtain biennial third-party assessments of its compliance with data privacy regulations, but neither confirmed nor denied liability.

LabMD . As we highlighted in our 2016 Year-End Update , the now-defunct medical testing laboratory LabMD appealed an FTC order finding that the company failed to reasonably protect its customers' personal information from data breaches and requiring it to establish a comprehensive information

security program to safeguard against such breaches in the future. [3] In 2008, billing information for approximately 9,300 consumers became accessible on a peer-to-peer network, and other personal information for at least 500 consumers ended up in the hands of identity thieves. [4] The FTC's order overturned the initial ruling of its own Administrative Law Judge, which had dismissed the Commission's charges because they failed to show that the company's conduct created a probability of harm. [5] In November 2016, the Eleventh Circuit granted the company's request for a stay pending appeal of the Commission's decision, [6] and this past June the court heard oral argument in the case. The Eleventh Circuit's ruling could significantly reshape the FTC's authority to regulate data privacy harms. At issue in the oral argument was whether the FTC must show proof of actual consumer harm to bring a data security enforcement action under Section 5 of the FTC Act. LabMD argued that the FTC overstepped its enforcement authority because no consumer suffered an actual injury as a result of the company's data breach. The FTC countered that it nevertheless could exercise its enforcement authority under Section 5 because the unauthorized exposure of health care information constitutes a substantial injury under traditional principles of privacy tort law. The panel was expected to issue a ruling in the months after the oral argument, but it has not yet done so.

D-Link . In January 2017, the FTC filed suit against the network equipment manufacturer D-Link Corp. over the company's allegedly inadequate security measures in its routers and internet cameras. [7] In its complaint, the FTC alleged that the company's failure to properly secure its routers and cameras left consumers vulnerable to hackers, particularly through their live video and audio feeds. Further, the complaint alleged that the company misled consumers by advertising on its website that its products are "Easy to Secure" and contain "Advanced Network Security." In September, the district court granted in part and denied in part the company's motion to dismiss the FTC's complaint. [8] The district court's ruling may have a dramatic impact on the FTC's ability to bring claims against companies for putting consumers' information at risk. The court found that three of the complaint's six counts were pled inadequately or with insufficient particularity, and gave the FTC until late October to re-plead its claims. Specifically, the court found that, for the three dismissed claims, the FTC failed to adequately plead harm because it relied "solely on the likelihood that [D-Link] put consumers at 'risk' because 'remote attackers could take simple steps, using widely available tools, to locate and exploit defendants' devices, which were widely known to be vulnerable,'" [9] and that this amounts to "a mere possibility of injury at best." [10] D-Link submitted its amended answer on October, and fact discovery is ongoing.

Vizio . In February 2017, TV manufacturer Vizio Inc. entered into a settlement with the FTC and the New Jersey Attorney General over allegations that it secretly gathered users' viewing data and shared it with third parties. [11] The settlement is significant given the increasing ubiquity of so-called "smart" devices, from televisions to thermostats to electronic assistants. Specifically, the regulators alleged that beginning in February 2014, Vizio began collecting second-by-second information about the content displayed on its "smart TVs," including content from cable, broadband, set-top boxes, streaming devices, and DVDs. Vizio allegedly appended this information with its users' personal information, such as users' age, sex, income level, marital status, household size, education level, home ownership, and home value. Vizio would then sell this information to third parties. As part of the settlement, Vizio agreed to pay $2.2 million and overhaul its data collection practices, as well as delete data obtained prior to March 1, 2016, and obtain affirmative consent from consumers regarding the company's data collection practices. Notably, Acting Chairwoman Maureen Ohlhausen issued a concurring statement expressing

skepticism that Vizio's conduct caused, or was likely to cause, a substantial injury to consumers. As part of the settlement, Vizio neither admitted nor denied liability.

Lenovo . In September 2017, the FTC announced that it had entered into a settlement, along with 32 state Attorneys General, with Lenovo Inc. over allegations that the company preloaded some of its computers with invasive software that compromised consumers' privacy and security. [12] The Commission alleged that, beginning in August 2014, Lenovo began selling laptops in the U.S. with a software program called VisualDiscovery, created by a company called Superfish, Inc., that would access consumers' personal information transmitted via the internet, such as login info for websites, Social Security numbers, medical information, and financial and payment information. The software would then send some of this information to the software company's servers, where the information was allegedly stored insecurely. This settlement is significant given the high value digital companies place on leveraging data regarding consumers' preferences to target their advertisements. As part of the settlement, Lenovo must get consumers' affirmative consent before preinstalling this sort of software; must implement a comprehensive software security program, which is subject to third-party audits for a period of 20 years; and must pay $3.5 million to state regulators. Lenovo neither admitted nor denied liability as part of the settlement.

b. Data Breach Guidance

With the arrival of the Trump administration, and 3 open seats on the Commission, companies and commentators have been watching carefully for any signal of whether, and how, the FTC's regulatory focus and enforcement priorities will change in coming years. Several recent statements provide some indication—albeit not definitive answers—about what the future may hold under the Trump administration.

In September, Acting FTC Chairwoman Maureen Ohlhausen said during a speech at the Federal Communications Bar Association that the FTC should focus on "substantial consumer injury" in determining which cases to pursue, rather than "hypothetical" harms. [13] "Government does the most good with the fewest unintended side effects when it focuses on stopping substantial consumer injury instead of expending resources to prevent hypothetical injuries," Ohlhausen said. "So understanding consumer injury in the context of privacy and data security is very important for the commission." [14]

While the FTC thus seems poised to cede some regulatory ground by moving away from regulating speculative harms, Acting Chairwoman Ohlhausen has also signaled that the Commission may adopt a broader definition of what constitutes a "substantial" injury. In a speech at a cybersecurity event at the Georgetown University Law Center in May, Ohlhausen noted that the FTC historically has focused on direct financial harms to consumers, but that this understanding may be too narrow. [15] Health and safety risks, such as those posed by the sharing of real-time and highly accurate location data that may leave consumers vulnerable to stalking, could also constitute a substantial injury, as could the disclosure of sensitive medical information. Whether Joseph J. Simons, whom President Trump in October announced that he intended to nominate to head the FTC, will take positions similar to those of Acting Chairwoman Ohlhausen is yet to be seen.

In her September speech, Ohlhausen announced a December workshop at which the FTC would examine the consumer harms that stem from informational injury. Leading up to the workshop, a host of pro-business groups including the U.S. Chamber of Commerce, the Association of National Advertisers, and the Retail Industry Leaders Association, issued public comments urging the Commission to adopt a regulatory framework designed to regulate actual injuries, rather than conjectural ones. [16] In contrast, several consumer groups such as the Electronic Privacy Information Center, encouraged the FTC to focus on the rise in data breaches and the concomitant increased risk of identity theft. The workshop took place on December 12, but the FTC has not yet announced any shifts in enforcement priorities as a result.

c. Scope of Authority—Common Carriers

As we mentioned in our last update, in May the Ninth Circuit granted the FTC's petition to rehear *en banc* a dispute between the Commission and AT&T over the company's allegedly deceptive "data throttling." [17] AT&T argued that it was not subject to the FTC's authority because it is a common carrier, a category that Section 5 of the FTC Act excludes from the FTC's jurisdiction. In August 2016, a Ninth Circuit panel agreed with AT&T that, because the company engaged in non-common carrier activities such as providing consumers with mobile data and email services, it fell outside the Commission's regulatory ambit.

The full Ninth Circuit held oral argument in September but has not yet issued a ruling. An affirmance could significantly curtail the FTC's jurisdiction.

2. Department of Health and Human Services ("HHS")

The flurry of HHS activity in 2016 related to the protection of patient privacy continued in 2017. As HHS continued the second-phase of its audit program to assess compliance with patient privacy provisions of the Health Insurance Portability and Accountability Act ("HIPAA"), [18] HHS also announced several multimillion-dollar settlements with health care companies for alleged HIPAA violations.

Matching the largest-ever HIPAA-related settlement, Memorial Healthcare Systems agreed to pay $5.5 million and implement a "robust corrective action plan" to settle claims that its employees had improperly accessed and disclosed information for over 115,000 patients. [19] HHS alleged that Memorial Health Care Systems failed to implement and manage user access rights and, despite results of previous risk analyses, failed to regularly review information system activity by employees and users at affiliated physician practices on applications that maintain protected information.

HHS also fined Children's Medical Center of Dallas $3.2 million for alleged HIPAA violations after two data breaches involving lost or stolen devices that contained unencrypted patient medical information. [20] The investigation by the Office for Civil Rights ("OCR") found that the medical center failed to implement risk management plans and failed to use encryption on its devices despite previous warnings to do so.

In addition, St. Luke's Roosevelt Hospital Center Inc. agreed to a settlement and corrective action plan following a complaint alleging that the hospital had faxed sensitive information concerning a patient's HIV status. [21] Although the total settlement amounted only to $387,000, the agreement stemmed from only two disclosures of Protected Health Information ("PHI"), highlighting the potential impact of even seemingly limited events.

HHS also announced several "firsts" in its HIPAA enforcement efforts, including the first enforcement action involving delayed reporting of a patient information breach and the first settlement with a wireless services provider. In the former, Presence Health agreed to pay $475,000 and revise its policies governing the privacy of patient information following allegations that it failed to properly notify more than 800 of its patients within 60 days of discovering that their personal information had been stolen. [22] In the latter, CardioNet, which provides remote mobile monitoring for patients at risk for cardio arrhythmias, agreed to pay $2.5 million and implement a corrective action plan for the alleged disclosure of unsecured electronic protected health information ("ePHI") after an employee's laptop was stolen from a parked vehicle. [23] OCR found that CardioNet had insufficient risk analysis and risk management processes in place at the time of the theft, as well as a lack of final policies and procedures implementing ePHI safeguards and the HIPAA Security Rule.

Closing out the year, HHS OCR announced that 21st Century Oncology, Inc. agreed to pay $2.3 million and adopt a comprehensive corrective action plan to settle alleged violations of the HIPAA Privacy and Security Rules that were uncovered after a hacker gained access to more than 2.2 million patient records, some of which were later sold to undercover agents from the FBI. [24]

Finally, following Acting HHS Secretary Eric Hargan's declaration of the opioid crisis as a public health emergency, HHS issued guidance regarding the circumstances in which health care providers may share a patient's PHI with family members, friends, or legal representatives. [25] Focusing on patients who are in crisis or incapacitated, such as during an opioid overdose, the guidance interprets current HIPAA regulations as allowing health care providers to share information in certain emergency or dangerous situations, including with persons who are in a position to prevent or lessen a serious and imminent threat to a patient's health or safety. The guidance also discusses factors to consider in assessing a patient's decision-making capacity and provides direction on health care providers' ability to share PHI in different situations, including when unable to obtain a patient's consent and after the patient has had an opportunity to object.

3. Securities and Exchange Commission ("SEC")

a. Cybersecurity Focus

In 2017, the SEC maintained the previous year's focus on cybersecurity incidents with respect to both its external oversight responsibilities and the internal operations of the agency. Since the issuance of its cybersecurity guidance in 2011, the SEC has continued to emphasize proper communications regarding cybersecurity issues within a company's management as well as proper disclosure of cybersecurity risks by registrants. [26]

The SEC announced in November that it will likely issue new guidance to public companies regarding disclosure and reporting of cybersecurity incidents. [27] Signaling this potential guidance, Acting Enforcement Director Stephanie Avakian stated in April that she could "absolutely" envision circumstances where enforcement would be necessary in light of a company's failure to report cyber incidents and risks. [28] The new guidance may also include provisions encouraging companies to consider how they handle stock sales by corporate insiders around the time of a cybersecurity breach. [29] In November, Director of the SEC's Division of Corporate Finance, William Hinman, stated, "it would be wise for folks to re-examine their insider trading policies." [30]

Two cybersecurity incidents with potential insider trading consequences that may influence the SEC's new guidance were disclosed in the fall of 2017. After Equifax discovered its massive breach in July—but before it was publicly reported in September—Equifax executives sold nearly $2 million in company stock. [31] Once the news of the breach broke, stock prices dropped significantly. [32] While the SEC has not confirmed or denied any SEC investigation of the executives for insider trading, Equifax reported in its third quarter 10-Q that the SEC had subpoenaed the company "regarding trading activities by certain employees in relation to the cybersecurity incident." [33] The second incident occurred this fall when the SEC faced its own cybersecurity threat. On September 20, 2017, as part of its "Statement on Cybersecurity," the SEC disclosed that a 2016 intrusion into EDGAR, the Commission's electronic filing system for public company disclosures, may have allowed hackers to gain access to and trade on the basis of the non-public information exposed. [34] The SEC stated it did not believe the intrusion was the result of a systemic risk or that it led to the exposure of any personally identifiable information. [35] Days after the statement, the SEC announced the establishment of a Cyber Unit to "focus on targeting cyber-related misconduct." [36]

b. Cyber Unit's First Charges

On December 4, 2017, the SEC announced the first charges filed by the newly established Cyber Unit. [37] The SEC's complaint alleges that Dominic Lacroix and his company, PlexCorp, operated an Initial Coin Offering ("ICO") fraud that raised over $15 million from investors by selling a security called PlexCoin, a cryptocurrency, and promising a 1,354 percent profit in less than one month. [38] The charges filed against PlexCorp, Lacroix, and his partner Sabrina Paradis-Royer [39] include violations of the anti-fraud provisions contained in Section 10(b) of the Exchange Act and Rule 10b-5, Section 17(a) of the Securities Act, as well as registration provisions in Sections 5(a) and 5(c) of the Securities Act. [40] The district court issued an emergency order freezing the assets of the company and the executives charged, and the SEC is seeking permanent injunctions and disgorgement plus interest and penalties. The SEC is also seeking a Final Judgment prohibiting the two executives from offering digital securities in the future. [41]

4. Federal Communications Commission ("FCC")

a. FCC Rulemaking

i. FCC Privacy Regulations for Broadband Providers Repealed

On April 3, 2017, President Trump signed a resolution repealing FCC privacy rules adopted in the prior year. [42] In 2016, the FCC adopted sweeping new regulations governing the ways in which providers of broadband Internet access service use and share their customers' personal information. [43] There were three key components to the regulations for broadband providers: (1) notice to consumers of data collection and use policies; (2) an opt-out provision for "non-sensitive" information used or shared by the providers and a requirement to obtain affirmative opt-in consent before they can use or share "sensitive" customer data; and (3) more stringent and specific requirements for notification of any data breaches. The resolution was passed under the Congressional Review Act, which allows Congress to repeal agency rules through simple majority votes.

ii. FCC Approves Next-Gen Broadcasting Technology

On November 16, 2017, the FCC voted 3-2 to permit the use of a new broadcast transmission standard, known as ATSC 3.0 or Next Gen TV. This new broadcast standard will allow more precise geolocating of television signals, ultra-high definition picture quality, more interactive programming, and localized safety warnings that have the ability to turn on televisions as necessary to transmit emergency broadcasts. [44] Privacy advocates argue that ATSC 3.0 allows broadcasters to collect data on viewing habits, spurring user-targeted ads similar to those on the Internet. During a House Communications Subcommittee FCC oversight hearing in November, Representative Debbie Dingell requested that the FCC address the types of information broadcasters will be able to collect from consumers and how it will be handled and protected. [45]

b. Cell Phone Cybersecurity

On August 24, 2017, the FCC's Public Safety and Homeland Security Bureau released Public Notice DA 17-799. This Notice was a result of Congress asking the FCC to tackle "fundamental security threats" to cell phones, since Congress felt current oversight by police and private entities "neither adequately addressed these serious cybersecurity vulnerabilities nor warned its customers about the risks they face." The Notice encourages communications service providers to implement recommended security countermeasures to prevent exploitation of carrier Signaling System 7 ("SS7") network infrastructure. [46] According to the Notice, security vulnerabilities present within SS7 networks allow attackers to obtain subscriber information, eavesdrop on subscriber traffic, engage in financial theft, and conduct denial-of-service attacks. The March 2017 recommendations for best practices to reduce SS7 security risks include: (1) awareness and protection, which covers the set of industry recommendations that advocate increased awareness of SS7 signaling and protective measures that can be deployed by telecommunication service providers; and (2) security best practices, which covers the set of industry recommendations that deal with best security best practices for SS7 communications.

c. FCC Settlements / Enforcement

i. $100M Settlement for Squatting on Spectrum Licenses

On January 12, 2017, a wireless spectrum trading company settled a dispute with the FCC over allegations it lied about its buildout of wireless infrastructure for $100 million and possible divestment from its spectrum licenses. [47] Because wireless spectrum is a scarce public resource, the FCC requires companies that license spectrum to put it to good use. In 2013 and 2014, the spectrum company received licenses in the 28GHz and 39GHz bands, which are identified for use in the next generation of cellular network, on the condition that it use them to provide services. [48] A November 2015 anonymous report alleged that the company never built several of the 39GHz systems it had told the FCC were completed. [49] As part of the settlement, the company agreed to pay a $100 million civil penalty, to surrender its licenses in the 39GHz spectrum, and to sell the remainder of its license portfolio.

ii. Robocall Fines

On June 22, 2017, FCC Chairman Ajit Pai stated that robocalls were the Commission's top enforcement priority. [50] That same day, the FCC voted to fine a Miami man a record-breaking $120 million for allegedly making 96 million spoofed robocalls to consumers in three months in violation of the Truth in Caller ID Act. [51] Spoofing refers to deliberately falsifying caller ID information to disguise an identity with the intent to harm or defraud consumers, or wrongfully obtain anything of value. The calls—which appeared to come from local numbers—purported to offer vacation deals from major companies like TripAdvisor, Expedia, and others. Consumers who "pressed 1" were transferred to foreign call centers where operators attempted to sell them timeshares. TripAdvisor alerted the FCC to the robocalls after fielding complaints from its customers. In July and August, the FCC levied fines of nearly $3 million and $82 million against other companies for unsolicited robocalls, the magnitude of the latter due in part to the targeting of vulnerable consumers, including the elderly, the infirm, and low income families. [52]

5. Consumer Financial Protection Bureau ("CFPB")

The CFPB was not particularly active in the area of data privacy and security in 2017. However, on October 18, 2017, the CFPB announced a series of non-binding Consumer Protection Principles to address the developing market for financial "aggregation services." [53] Such companies offer a broad range of products and services that are developed using consumer-provided financial data. This data is collected and aggregated by financial services companies, "fintech" firms, and other companies. The services offered range from the provision of financial advice to the facilitation of underwriting or fraud-screening. The release of the Principles followed a November 2016 Request for Information to stakeholders in the "aggregation services" market. The Principles, intended to protect consumers who authorize third parties to collect their financial data to provide these services, are not intended to alter or interfere with the scope of existing consumer protections in this market. The CFPB simultaneously released a summary of the stakeholder insights underlying the development of the Principles. [54] The CFPB identified the following nine principles that providers of "aggregation services" should follow, all of which are anchored by the core belief that users should retain control over their information: [55]

Access: Users should be able to request and obtain information about their ownership or use of a financial product or service from the provider.

Data Scope and Usability: The scope of financial data subject to consumer and consumer-authorized access includes, but is not limited to, information about any transaction and the terms of an account. Information should be made available in a usable format for consumers and consumer-authorized third parties.

Control and Informed Consent: Consumers should be entitled to a full and effective disclosure of the authorized terms of access, storage, use and disposal of information. Consumers should also be able to readily revoke authorization to access, use or store their data.

Authorizing Payments: A user's consent to the access of data does not constitute consent for payment authorization. Providers may request both types of authorization from a consumer requesting its services.

Security: Consumer data must be maintained securely. Parties with access to data must have adequate processes in place to protect against and effectively respond to data breaches.

Access Transparency: Users should be able to obtain information regarding the uses to which their information will be put and the parties to which it will be provided.

Accuracy: Consumer data gathered by "aggregation services" must be accurate and up-to-date.

Ability to Dispute and Resolve Unauthorized Access: Users should have the ability to dispute and resolve incidents involving unauthorized access and data sharing.

Efficient and Effective Accountability Mechanisms: Commercial participants should be incentivized to protect consumer-provided data, but also must be held responsible for any risks they introduce to consumers.

The agency emphasized that the Principles do not "establish binding requirements or obligations relevant to the Consumer Bureau's exercise of its rulemaking, supervisory, or enforcement authority." [56] Nor are they intended to "provide guidance on existing statutes and regulations that apply in this market." [57] Nevertheless, the CFPB stated that the Principles "express the Bureau's vision for realizing a robust, safe, and workable data aggregation market" and suggested that the Bureau "will continue to monitor closely developments in this market." [58] Thus, it is possible that as "aggregation services" and "fintech" firms become increasingly prevalent, the CFPB will become more involved with the regulation of data privacy-related issues.

6. State Attorneys General

State attorneys general play a key role in data privacy and security matters. During the past year, state attorneys general were at the forefront of concerted efforts to bring enforcement actions and develop privacy and cybersecurity regulations.

a. Collaboration Among Attorneys General

During the past year, states increasingly coordinated their enforcement efforts with each other and with other government agencies to settle multi-state litigations involving mega-data breach cases. In May 2017, the Target Corporation ("Target") reached an $18.5 million settlement—the largest state data breach settlement in history—with 47 states and the District of Columbia. The settlement brought an end to investigations jointly led by state attorneys general into Target's November 2013 data breach involving unauthorized access to portions of Target's computer systems that process payment card transactions at Target's retail stores and to portions that store Target customer contact information. [59] Under the terms of the agreement, Target will be required to develop, implement, and maintain a comprehensive information security program, to hire a third party to conduct a security assessment, and implement additional administrative safeguards to further strengthen the company's data security. [60]

In August 2017, 33 state attorneys general reached a $5.5 million multi-state settlement with Nationwide Mutual Insurance Company ("Nationwide") and its wholly owned subsidiary Allied Property & Casualty Insurance Company ("Allied") over a 2012 data breach. [61] The personal information of 1.27 million people was stolen when hackers exploited a vulnerability in Nationwide/Allied's web application hosting software—a vulnerability that allegedly could have been remedied with a previously available software patch that Nationwide/Allied had failed to apply. [62]

As described more fully above, in September 2017 Lenovo reached a $3.5 million multi-state settlement to resolve charges brought by 32 state attorneys general and the FTC. [63] Of the 23 states involved in the settlement, California received the largest share, amounting to $389,204, based largely on its size and leadership role in the investigation. [64]

Following the public announcement of the Equifax breach in September, Massachusetts became the first state to sue Equifax, claiming that Equifax failed to maintain the appropriate safeguards to protect consumer data, despite being aware of the vulnerabilities in its system for months. [65] On November 30, 2017, the Judicial Panel on Multidistrict Litigation held a hearing on the pending motion to consolidate and transfer the numerous cases filed (and cases to be filed in the future) against Equifax to the U.S. District Court for the Northern District of Georgia, near the company's headquarters in Atlanta. [66]

b. Developments Within States

The California Attorney General settled a number of data breach and consumer protection cases. On November 22, 2017, the Attorney General settled a case with Cottage Health System ("Cottage Health") and its affiliated hospitals to resolve allegations resulting from two separate and unrelated data breach incidents in 2013 and 2015. [67] The Attorney General alleged that Cottage Health failed to implement basic, reasonable safeguards to protect personal medical information, in violation of California's Confidentiality of Medical Information Act, Unfair Competition Law, and HIPAA. [68] Under the terms of the settlement, Cottage Health agreed to update its security measures and pay a $2 million penalty. [69] Cottage Health was also required to hire a data privacy security officer to ensure it

develops and follows appropriate procedures, as well as to begin completing annual privacy risk assessments. [70]

The New York Attorney General's Office remained active in combatting violations of data security. On October 31, 2017, the New York Attorney General, along with the Vermont Attorney General, reached a $700,000 settlement with Hilton Domestic Operating Company, Inc., formerly known as Hilton Worldwide, Inc. ("Hilton") as a result of two separate data security incidents in 2015 which exposed credit card numbers. [71] The investigation allegedly revealed that Hilton did not adequately protect consumers' information and failed to provide timely notice of the breach, as New York General Business Law § 899-aa(2) requires notice to customers in the "most expedient time possible and without unreasonable delay." [72] The reached settlement, among other things, requires Hilton to maintain a comprehensive information security program designed to protect consumer cardholder data and to conduct annual data security assessments.

As noted earlier, on February 6, 2017 the New Jersey Attorney General reached a settlement agreement with Vizio, Inc., a smart TV maker, for alleged violations of consumer protection laws by collecting and sharing data on the viewing habits of its smart TV users without their consent. [73] Vizio agreed to pay $2.2 million and to change its data collection practices to resolve allegations, ending parallel investigations conducted by the Attorney General and the FTC. [74] The state obtained $1 million and the FTC obtained $1.5 million in the settlement. [75]

The Washington Attorney General released its second edition of the *Annual Data Breach Report*, containing a summary of the data collected from the data breach notifications required by Washington's notification laws. [76] Since the 2015 amendment to Washington's data breach laws, the Attorney General has actively enforced compliance with the state's notification regulations.

7. New York Department of Financial Services ("NYDFS")

In 2017, New York's Department of Financial Services ("NYDFS") adopted groundbreaking regulations that broadly regulate cybersecurity within the financial services industry. NYDFS is the New York state regulator of financial services licensed in the state and thus supervises many large banks and insurance companies. Effective March 1, 2017, the NYDFS regulations require banks, insurance companies, and other financial services institutions subject to regulation by the NYDFS to establish and maintain a comprehensive cybersecurity program. [77] "Covered Entities" are required, among other things, to perform a risk assessment to assess their cyber risks, implement a written cybersecurity policy, and maintain a comprehensive cybersecurity program. [78] While some security measures were mandated by August 28, 2017, others are mandated by September 3, 2018, with a final compliance date of March 1, 2019. [79]

The final regulations, codified in 23 NYCRR Part 500, are largely the same as the proposed rules discussed in last year's 2016 Year-End Update , but differ in the following key ways:

- Cybersecurity programs must be based on the risk assessment performed by each Covered Entity.
- Risk assessments must be performed "periodically" instead of "annually."

- The company's cybersecurity plan can be reviewed by either a senior officer or the board of directors, but does not need to be reviewed by both.
- Covered Entities must hold records, schedules, and data supporting the certificate of compliance for five years, and make this documentation of compliance available to NYDFS upon request. However, the record retention for audit trails designed to detect and respond to cybersecurity events is limited to three years.
- There is a limited small business exemption for Covered Entities that have fewer than ten New York employees and less than $5 million in gross annual revenue or under $10 million in year-end total assets.
- The Chief Information Security Officer ("CISO") does not need to be an internal employee, but instead can be employed by the Covered Entity, one of its affiliates or a third-party service provider.
- Companies do not need to encrypt nonpublic information in transit over external networks if doing so is "infeasible." Instead, they may secure the information using "alternative compensating controls reviewed and approved" by the CISO. [80]

This fall, Governor Cuomo directed the NYDFS to extend the regulations to credit bureaus, expanding the reach of both the rules and the NYDFS itself, which had not previously had oversight over credit reporting agencies. Under the proposed regulation, all consumer credit reporting bureaus that operate in New York must register with the NYDFS annually, beginning on or before February 1, 2018. The compliance schedule will begin on April 4, 2018. [81]

8. Trump Administration Actions

a. Presidential Executive Order

On May 11, 2017, President Trump issued an executive order entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which lays out the administration's priorities in three areas of focus: (1) cybersecurity of federal networks, (2) cybersecurity of critical infrastructure, and (3) cybersecurity of the nation. [82] The order directed a thoroughgoing review of existing policies regarding cybersecurity in a variety of different sectors.

For cybersecurity of federal networks , the Executive Order stated that the President would hold agency heads accountable for managing the cybersecurity risks to their agencies, and directed them to use *The Framework for Improving Critical Infrastructure Cybersecurity*, developed by the National Institute of Standards and Technology, to manage cybersecurity risk. [83] The Executive Order also directed the agency heads to submit a risk management report to Homeland Security and the Office of Management and Budget ("OMB") within 90 days, outlining their existing risk mitigation strategies and each agency's action plan to implement the Framework, and then contemplated that the Director of the OMB would submit its own determination to the President within 60 days. [84]

The Executive Order also articulated the administration's policy to "build and maintain a modern, secure, and more resilient executive branch IT architecture," directing the Director of the American Technology Council—created by the President on May 1, 2017—to coordinate a report on the feasibility of transitioning all agencies to "one or more consolidated network architectures" or to "shared IT services." [85] The American Technology Council issued a detailed report to the President on federal IT modernization in the fall of 2017, and delivered the final Federal IT Modernization report on December 13, 2017. [86]

For cybersecurity of critical infrastructure , the Executive Order stated the administration's policy to "support the cybersecurity risk management efforts of the owners and operators" of critical infrastructure. [87] First, it directed the Secretary of Homeland Security to coordinate with other senior administration officials to identify the greatest risk of attacks to infrastructure that could result in wide-scale effects on public health, economic security or national security, and to deliver a report setting forth its findings and recommendations within 180 days. [88] Second, it directed the Secretary of Homeland Security to work with the Secretary of Commerce to determine whether existing federal policy sufficiently promotes "market transparency of cybersecurity risk management practices." [89] Third, it directed the Secretary of Homeland Security with the Secretary of Commerce to work together with "appropriate stakeholders to improve the resilience of the internet and communications ecosystem" to "threats perpetrated by automated and distributed attacks (e.g., botnets)." [90] In response to the Executive Order, on January 5, 2018, both agencies released for public comment a report on enhancing the resilience of the Internet and communications ecosystem against botnets and other automated, distributed threats. [91] Fourth, it directed the Secretary of Energy and the Secretary of Homeland Security to coordinate with state and local governments to prepare an assessment of the Nation's vulnerability to prolonged power outages resulting from cyber incidents. [92] Fifth, it directed the Secretary of Defense, again in coordination with the Department of Homeland Security, to prepare an assessment of the risks facing the defense industry. [93]

For cybersecurity for the nation , the Order states the administration's policy to ensure that the internet "remains valuable for future generations." [94] First, the Order directs various agencies to prepare a report to the President "on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats." [95] Second, the Order directs agency heads to prepare a report on the agencies' "international cybersecurity priorities" to the Secretary of State, who would then prepare a report "documenting an engagement strategy for international cooperation in cybersecurity." [96] Finally, the Order solicits three different reports in the area of "workforce development," focused on the education and development of an American cybersecurity workforce, on the United States' competitiveness with peer programs in other countries, and on the United States' national-security-related cyber capabilities. [97]

Although the release of the Executive Order was met with praise across party lines, critics in the months since it was released have noted gaps in its implementation. To date, it is unclear which federal agencies have complied with the review process set forth in the Executive Order, and in September 2017, a commentator observed that "the goal of a speedy review process . . . ha[d] not materialized." [98] The administration has seen some turnover in cybersecurity-related posts. [99] In December 2017, the

administration affirmed that cybersecurity remained a key priority and suggested that it would build on the Executive Order by releasing a new strategy for cybersecurity. [100]

b. Release of the Vulnerabilities Equities Process ("VEP")

On November 15, 2017, the Trump administration publicly disclosed the Vulnerabilities Equities Process ("VEP"), a set of guidelines used by government agencies and departments to determine when to inform market actors of security vulnerabilities in their software and hardware. [101] The unclassified document states that the purpose of the VEP is to "balance[] whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge . . . for national security and law enforcement." [102] The VEP describes an Equities Review Board for interagency deliberation, consisting of representatives from several government agencies, with the National Security Agency ("NSA") serving as the VEP Executive Secretariat. [103] Generally, an agency that learns of a vulnerability will submit information regarding the vulnerability, together with a recommendation whether to disseminate or restrict the vulnerability, to the VEP Executive Secretariat once the vulnerability reaches a certain threshold. [104] The VEP Executive Secretariat then notifies points of contacts at relevant agencies. Interested agencies then state whether they concur with the recommendation to disseminate or restrict the vulnerability. [105] The VEP states that the purpose of distributing information is to obtain a consensus regarding dissemination or restriction, but also provides procedures for resolving contested preliminary determinations. [106] The VEP outlines the considerations that bear on determining whether to disseminate or restrict information regarding a vulnerability. [107]

B. Legislative Developments

1. Federal Developments

Last year did not see much congressional legislation in the area of cybersecurity. The most significant piece of privacy legislation to reach President Trump's desk was not new legislation, but a repeal of FCC broadband provider privacy rules that were set to take effect at the end of 2017. In addition to rolling back the FCC broadband rules, Congress also took steps toward addressing foreign surveillance, cybersecurity, and data breach notification, but as of the date of this review, few of those bills have yet to become law.

a. Repeal of Broadband Privacy Rules

In March 2017, both the House and Senate passed resolutions under the Congressional Review Act to repeal FCC broadband privacy rules that were set to take effect at the end of 2017. Entitled "Protecting the Privacy of Customers of Broadband and Other Telecommunication Services," 81 Fed. Reg. 87274 (December 2, 2016), the rules would have imposed certain privacy regulations on internet service providers ("ISPs"), such as requiring them to provide adequate privacy notices and comply with data breach notification requirements. The most controversial of these rules was the requirement that ISPs obtain consumers' opt-in consent before sharing consumer information (such as browsing history) with third parties, as certain commentators argued that the proposed rules placed ISPs at a disadvantage when compared to other online companies such as Google and Facebook. [108] FCC Chairman Ajit Pai stated

his support for the repeal in part on the belief that the rules "were designed to benefit one group of favored companies." [109] Chairman Pai's announcement also indicated that the FCC will "be working with the FTC to restore its authority to police internet service providers' privacy practices," and to "end the uncertainty and confusion that was created in 2015 when the FCC intruded in this space." [110] On April 3, 2017, President Trump signed the repeal into law. [111]

b. Foreign Surveillance

With Section 702 of the Foreign Intelligence Surveillance Act ("FISA") [112] initially set to expire at the end of 2017, there has been significant debate over the appropriate scope of the U.S. government's foreign surveillance powers. Section 702 allows the U.S. government to gather foreign intelligence information without a warrant, subject to certain restrictions. [113] Even before legislation on this topic was introduced, government and industry groups began advocating for their respective positions. For example, on April 18, 2017, the Office of the Director of National Intelligence released a report supporting a reauthorization of Section 702, including controversial aspects such as "upstream" collection whereby the "NSA obtains communications directly from the Internet backbone, with the compelled assistance of companies that maintain those networks." [114] With the deadline for reauthorization approaching, the House Judiciary Committee introduced the FISA Amendments Reauthorization Act of 2017 to renew Section 702 for four years while making "key reforms" to the program to "strengthen privacy protections for Americans." [115] The Senate Intelligence Committee also advanced a reauthorization bill. [116] The White House and Congress subsequently pushed the deadline for reauthorization from December 31, 2017 forward to January 19, 2018. [117] On January 11, 2018, the House of Representatives voted to extend Section 702 for six years with minimal changes, rejecting a push by a bipartisan group of lawmakers to impose privacy limits on the U.S. government's ability to gather emails and other personal communications. [118] The Senate approved the FISA reauthorization bill on January 18, 2018, [119] and President Trump signed the bill into law on January 19, 2018. [120] FISA is now set to expire in December 2023. [121]

c. Email Collection by Law Enforcement

Congress continues to introduce legislation to reform the Electronic Communications Privacy Act ("ECPA"), [122] but has yet to finalize a bill for the President's signature. ECPA addresses, among other issues, procedures for law enforcement to obtain stored electronic communications. For example, ECPA currently requires only a subpoena for the U.S. government to collect emails over 180 days old, while emails under 180 days old require a warrant. In February 2017, the House unanimously passed a bill called the Email Privacy Act [123] to reform ECPA. [124] Among other changes, the House bill would require a warrant to obtain emails over 180 days old. In July 2017, Senators Patrick Leahy and Mike Lee proposed the ECPA Modernization Act, a Senate version of ECPA reform. [125] The ECPA Modernization Act marks the third time in five years that the bipartisan team has attempted to reform the ECPA. The bill currently languishes in the Senate.

d. Cybersecurity and Data Breach Notification

In 2016 the House and Senate each passed legislation related to cybersecurity without finalizing any bills to be signed into law. This past year, Congress similarly attempted to address cybersecurity measures with limited success in enacting new law. For example, on May 16, 2017, the House overwhelmingly passed the Strengthening State and Local Cyber Crime Fighting Act of 2017, which formalizes the Secret Service's National Computer Forensic Institute as the entity responsible for coordinating investigations into cyberattacks and other computer hacking, as well as providing training to state and local agencies on dealing with cybercrimes. [126] After the Senate passed a version of the same bill, President Trump signed the bill into law on November 2, 2017. [127]

Following the Equifax data breach, the Senate and House have been considering the Consumer Privacy Protection Act of 2017. [128] The bill requires that companies report data breaches "as expediently as possible" or face civil penalties. Congress has previously considered similar bills, however, without adopting a nationwide data breach notification standard. [129] Thus data breach notification requirements continue to vary among the 48 states that have adopted laws on the subject. [130]

2. State Developments

In 2017, at least 42 states introduced over 240 bills related to cybersecurity and data privacy. [131] Key areas of legislative activity include ISP data collection and tracking, data breach notification, cybersecurity committees, computer crimes, employee monitoring notice, and cybersecurity training.

a. ISP Data Collection and Tracking

A number of states introduced legislation requiring ISPs to obtain consumer consent before gathering and sharing online data with third parties. This flurry of legislative activity comes on the heels of Congress's rollback of FCC regulations that were poised to expand online privacy rules and to require ISPs to notify customers before selling data to a third party. [132] While only Nevada and Minnesota have actually passed privacy laws protecting consumers' data privacy in the wake of the now-repealed FCC regulations, nearly 30 other states have introduced similar legislation. Both Nevada's and Minnesota's legislation prohibit disclosure of personal identifying information to third parties. Beyond personal identifying information, Minnesota's legislation also requires ISPs to obtain permission before disclosing subscribers' online usage and browser history. Common features across other state bills include requiring consent before collecting customers' personal identifying information, specifying the form of ISP data collection notice, and prohibiting discounts for customers who consent to their personal identifying information being shared with third parties. In California, a recent ballot initiative would impose even greater restrictions, by requiring medium and large-sized businesses and ISPs to compile and maintain detailed records of disclosed consumer information and requiring ISPs to maintain the same level of service for all customers—regardless of whether they opt out of information-sharing. [133] Beyond these common features, all of the proposed legislation in this area varies as to the liability extended beyond ISPs, including website operators, as well as the form of consent that must be given before gathering and sharing consumer data.

b. Data Breach Notification

Forty-eight states—and the District of Columbia, Guam, Puerto Rico, and the Virgin Islands—have now passed legislation requiring both private companies and government entities to notify individuals regarding security breaches of personal identifying information. Alabama and South Dakota are the only two exceptions. Since our last update, New Mexico passed legislation on April 6, 2017, effective June 16, 2017, requiring notification upon the unauthorized acquisition of personal identifying information. [134] Delaware took legislative action to expand its definition of "personal identifying information," to include, in addition to the usual triggers like passport numbers and state identification card numbers, health insurance policy numbers or other health insurance identifiers, medical history or diagnosis information, and DNA profiles. [135]

c. Cybersecurity Committees

Another trend in 2017 was the continued establishment of state committees on cybersecurity. Four states—Georgia, Massachusetts, North Carolina, and Pennsylvania—introduced bills to form cybersecurity committees to study and improve cybersecurity preparedness and enhance state-wide responses to security threats. Illinois introduced legislation that would form an International Cybersecurity Task Force to review reports from the Department of Homeland Security and the FBI on "Russian Malicious Cyber Activity" and develop strategies to implement or reject the recommendations espoused by those reports. [136] Puerto Rico also enacted legislation directing the Senate and House Committees on Public Safety to research computer security with an eye towards understanding how new technologies might help ensure the proper handling of confidential information. [137]

d. Computer Crimes

In 2017, states continued to pass legislation to target computer crimes, with increased penalties for such offenses. For example, Connecticut passed legislation establishing the crime of computer extortion by the use of ransomware as a felony. [138] This bill was introduced after the WannaCry attack, in which a ransomware worm targeted Microsoft Windows, disrupting the normal functions of numerous organizations, including hospitals, ambulances, health clinics, shipping companies, and schools. Connecticut's legislature framed the bill as a preventative measure to protect against and deter similar cyberattacks. Wyoming passed legislation to create the criminal offense of computer extortion, a felony punishable by a prison term of up to ten years and a fine of $10,000, and to expand the computer crimes to be investigated by Wyoming's division of criminal investigation. [139] A number of other states also introduced legislation concerning computer crimes that remains pending. For example, New Jersey introduced a bill that clarifies the scope of the crime of unlawful access to password-protected communications—limiting it to access that is "knowingly" without authorization—and provides for imprisonment terms of up to 18 months for the most serious version of this offense. [140] New York also introduced bills to provide for the calculation of damages caused by computer tampering, requiring that cyber terrorism be classified as a Class B felony [141] and increasing penalties for crimes involving the use of personal information, fraud, tampering, theft, and use of a computer to commit crimes. [142]

e. Notice of Monitoring Employee Communications and Internet Access

In 2017, a handful of states introduced legislation requiring private or government employers to notify employees before monitoring employees' email communications or Internet access and browsing histories. Specifically, Colorado and Tennessee passed legislation providing that government entities operating electronic mail communications systems must adopt written policies on monitoring activities that specify when employee correspondence may be considered a public record. [143] Connecticut and Delaware now require private and public employers to give notice to employees before monitoring employee email communications or Internet usage behavior. [144] The ramifications of non-compliance for Connecticut employers are civil penalties of $500 for the first offense, $1,000 for the second offense, and $3,000 for each subsequent offense. [145] The ramifications of non-compliance for Delaware employers are civil penalties of $100 per violation. [146]

f. Cybersecurity Training

This year, several states introduced legislation to improve state employee cybersecurity training. Illinois passed a bill that requires state employees to participate in annual training by the Department of Innovation and Technology to enhance cybersecurity preparedness. [147] New Jersey and Oregon introduced similar bills. [148] Relatedly, California introduced legislation that would direct the Regents of the University of California and other higher education institutions to evaluate their cybersecurity education and training programs to ensure that "the state is meeting the workforce needs of the cybersecurity industry." [149]

II. Civil Litigation

Privacy-related civil litigation was again prevalent in 2017, which witnessed one of the largest private data breaches in history. Numerous data breaches announced in 2017 led to civil actions, including actions on behalf of government entities. Courts grappled with issues related to standing post-*Spokeo*, approved settlements of numerous class action suits, and presided over shareholder derivative suits alleging that directors and officers breached their fiduciary duties in overseeing corporate cybersecurity.

In addition to breach-related litigation, plaintiffs filed multiple class action lawsuits alleging that technology companies violated state and federal laws by scanning user emails for targeted advertising and other business purposes. Last year also continued the recent trend of civil and criminal cases being brought against both businesses and individuals for recording phone calls without the requisite consent and against companies for violating the Telephone Consumer Protection Act ("TCPA") and the Video Privacy Protection Act ("VPPA"). Additionally, there was an increase in regulatory guidance and regulatory and private actions related to the "Internet of Things," *i.e.*, smart and connected devices.

A. Standing After *Spokeo*

1. Background

In 2017, litigation over standing often predominated in data privacy actions as a result of the Supreme Court's 2016 decision in *Spokeo, Inc. v. Robins*. [150] As discussed further in our 2016 Year-End

Update , the Supreme Court held in *Spokeo* that "a bare procedural violation" of a statute without a resulting "concrete" injury does not satisfy the "injury-in-fact" requirement of Article III standing. [151] The Court emphasized that "Article III standing requires a concrete injury even in the context of a statutory violation." [152]

We thus observed last year that, on its face, *Spokeo* seemed poised to favor defendants in data privacy litigation, but noted that lower courts' subsequent interpretation and application of *Spokeo* had been decidedly mixed. That trend continued in 2017, as appellate courts continued to split on the question of whether the risk of future identity theft stemming from data breaches that resulted in stolen personal information is enough to confer standing without present injury. Further, while courts continued to favor plaintiffs in cases brought under the Video Privacy Protection Act ("VPPA") and the Telephone Consumer Protection Act ("TCPA") in 2017, they often ruled for defendants on standing challenges in lawsuits concerning unlawful data retention.

2. Post-*Spokeo* Standing Decisions in Privacy Cases

a. Data Breach

Last year, the circuit courts diverged on the question of whether plaintiffs have standing to sue based on the possibility that they may become victims of identity theft following a data breach.

For example, in January 2017, the Third Circuit reversed a district court dismissal, finding that a putative class of customers sufficiently pled standing in a Fair Credit Reporting Act ("FCRA") case based on allegations that the defendant inadequately protected personal information stolen from that company. [153] The court agreed with the plaintiffs that the purported "violation of their statutory right to have their personal information secured against unauthorized disclosure constitute[d], in and of itself, an injury in fact," and that establishing standing did not require additional "specific harm," such as economic damages. [154] It further emphasized that the wrongful "dissemination of [the plaintiffs'] own private information" was "the very injury that FCRA is intended to prevent," rather than a *de minimis* technical infraction that would be insufficient under *Spokeo*. [155] Likewise, the D.C. Circuit found standing in a data breach case based on allegations that the plaintiffs "face[d] a substantial risk of identity theft" resulting from their stolen personal information. [156]

Conversely, in an unpublished decision, the Second Circuit affirmed dismissal of a suit predicated on alleged theft of credit card information, because the plaintiff failed to plead "a particularized and concrete injury suffered from the attempted fraudulent purchases," since she was never asked to pay for an unauthorized transaction. [157] Moreover, the court held that there was no risk of future harm because the "stolen credit card was promptly canceled after the breach and no other personally identifying information . . . [was] alleged to have been stolen." [158] The Fourth Circuit reached a similar conclusion in a data breach case concerning personal information obtained from veterans' medical care facilities after determining that the "threatened injury of future identity theft" was speculative rather than sufficiently imminent. [159] A number of district courts also dismissed data breach claims for lack of standing where the risk of prospective harm from a data breach was, in their view, hypothetical. [160]

The Eighth Circuit reached a split decision on the question of standing based on the possibility of identity theft following a data breach in *In re SuperValu, Inc.*, a multi-district litigation involving several putative classes that sued retail grocery stores that had suffered two cyber-attacks. [161] The plaintiffs alleged theft of their personal information and violations of, among other things, various state data breach notification statutes. [162] The Eighth Circuit agreed with the district court that the plaintiffs had failed to adequately plead injury based on the risk of future identity theft, and it noted that its sister circuits—as discussed above and in our last review—had reached "differing conclusions on the question of standing" in similar data breach cases. [163] Observing that "this out-of-circuit precedent . . . ultimately turned on the substance of the allegations before each court," the Eighth Circuit concluded that the plaintiffs in *SuperValu* had not plausibly alleged that the "defendants' data breaches create[d] a substantial risk that [the] plaintiffs [would] suffer credit or debit card fraud." [164] However, the court also found that one named plaintiff had sufficiently pled a present injury based on actual misuse of his credit card information, and it accordingly reversed the dismissal of that particular individual's claims. [165]

b. Unlawful Disclosure

Standing decisions in unlawful disclosure cases in 2017 turned on whether dissemination of the information at issue posed a material risk of harm to a plaintiff's statutory interests. In keeping with *Spokeo*, lower courts dismissed lawsuits predicated on *de minimis* procedural infractions.

After the Supreme Court vacated and remanded *Spokeo* for further consideration of whether the plaintiff had pled a concrete injury under the FCRA, the Ninth Circuit answered in the affirmative. [166] It held that the inaccurate information disclosed in the credit report at issue implicated "material facts" about the plaintiff's life and "could be deemed a real harm" to, *inter alia*, his employment prospects. [167] The Ninth Circuit similarly found standing in *Syed v. M-I, LLC*, an FCRA case concerning the alleged failure of an employer to inform job applicants that it would check their credit histories as part of the application process, [168] as well as in a VPPA action based on allegations that the defendant disclosed information about the plaintiff's video-watching habits. [169] In the latter decision, the court held that, "although the FCRA outlines *procedural* obligations that *sometimes* protect individual interests, the VPPA identifies a *substantive* right to privacy that suffers *any time* a video service provider discloses otherwise private information." [170] The Eleventh Circuit issued an identical ruling in another VPPA appeal. [171] A number of district courts also reached similar decisions in cases concerning failures to comply with the FCRA's and the Fair Debt Collections Practices Act's ("FDCPA") disclosure requirements. [172]

However, in contrast to *Syed*, the Seventh Circuit found in *Groshek v. Time Warner Cable, Inc.* that a plaintiff did not suffer "a concrete informational injury" under the FCRA based on a prospective employer's purported failure to properly obtain an applicant's permission before procuring a credit report. [173] The court distinguished *Syed* on the ground that the "Ninth Circuit had factual allegations from which it could infer harm, whereas" the plaintiff in *Groshek* "present[ed] no factual allegations plausibly suggesting that he was confused by the disclosure form or the form's inclusion of a liability release . . . ." [174] Likewise, in an FCRA class action based on a credit reporting agency's inclusion of a defunct credit card company on its reports, the Fourth Circuit found that the named plaintiff had failed to

demonstrate how he had been injured by the erroneous information and therefore had "suffered no real harm, let alone the harm Congress sought to prevent in enacting the FCRA." [175] Accordingly, the court vacated the judgment awarding damages to the class. [176] The Second Circuit similarly affirmed dismissals of two Fair and Accurate Credit Transactions Act ("FACTA") suits predicated on the disclosure of credit card information on restaurant and retail receipts after finding that the purported injuries did not pose a "material risk of harm" to the plaintiffs' statutory interests. [177] District courts have followed course in other FACTA actions. [178]

c. Unlawful Retention

Unlawful retention cases have continued to trend in defendants' favor on the question of standing. For instance, earlier this year in *Gubala v. Time Warner Cable, Inc.*, the Seventh Circuit determined that there was no standing in a Cable Communications Privacy Act ("CCPA") action based on allegations that the defendant had retained the plaintiff's personal information after the plaintiff canceled a cable subscription. [179] The court determined that there was no cognizable injury because the plaintiff failed to allege that the defendant had "ever given away or leaked or lost any of his personal information or intend[ed] to give it away or [was] at risk of having the information stolen from it." [180]

d. Unlawful Acquisition/Use

The courts have continued to split on the question of standing in unlawful acquisition and use cases. In *Santana v. Take-Two Interactive Software, Inc.*, for example, the Second Circuit affirmed the district court's dismissal of a Biometric Information Privacy Act ("BIPA") lawsuit predicated on the defendant's alleged unlawful collection, dissemination, and retention of biometric data used to create 3D models of players' faces in basketball video games, for lack of standing. [181] The court held that the purported BIPA violations were procedural and did not pose a "material risk of harm" to the plaintiffs' statutory interests sufficient to establish an Article III injury. [182] Conversely, over the past year, district courts found standing for a Wiretap Act claim predicated on use of a smartphone application to track users' physical movements, [183] as well as for VPPA, Wiretap Act, and state law claims based on the collection of video-viewing information through smart TVs. [184] Courts also found standing in the context of Driver's Privacy Protection Act claims stemming from the sale of vehicle accident reports containing personal information to third parties for solicitation purposes. [185]

e. TCPA Claims

In TCPA cases, courts have continued to find that unsolicited electronic communications constitute a concrete injury to statutory privacy rights. For example, the Ninth Circuit held that spam-like text messages about gym memberships violated "the substantive [TCPA] right to be free from certain types of phone calls and texts absent consumer consent," [186] and the Second and Third Circuits found that plaintiffs adequately alleged harm in actions based on unwanted, prerecorded telephone calls. [187] A number of district courts have reached identical conclusions in TCPA cases; [188] however, one court refused to certify a proposed TCPA class after determining that some prospective class members had consented to receive the calls at issue and thus did not suffer a cognizable injury. [189]

3. Looking Ahead

Spokeo did not provide a bright-line rule squarely prohibiting plaintiffs from suing for intangible injuries. Accordingly, lower courts have continued to grapple with its application in the data privacy space. There appears to be an emerging pro-plaintiff consensus in VPPA and TCPA actions, and courts have continued to favor defendants in retention suits. However, the circuit courts have adopted divergent views on whether data breaches resulting in stolen personal information and the associated risk of future identity theft are, by themselves, enough to confer standing absent allegations of present harm. On December 6, 2017, Spokeo again petitioned for certiorari and sought review of the Ninth Circuit's latest standing determination. [190] However, shortly before publication of this review, the Supreme Court rejected Spokeo's petition, [191] thereby declining the opportunity to clarify its precedent.

B. Data Breach Litigation

1. Litigation

a. High-Profile Breaches in 2017

Last year witnessed one of the largest data breaches in history, when it was reported that Equifax, Inc., one of the three major American credit bureaus, had its systems compromised, affecting more than 143 million Americans. But Equifax was not alone in suffering massive data breaches: for example, a white hat hacker revealed in July that a political data analytics company had left the voting information of nearly 200 million Americans exposed. Throughout the year hackers targeted government agencies and companies in every industry, seeking out personally identifiable information ("PII"), customer login information, payment information, and health care information, among others. Litigation quickly followed many of the announced breaches, including civil actions and suits on behalf of government entities.

i. Credit Bureau Attacks

In the Equifax attack, hackers were able to access names, Social Security numbers, addresses, and other PII, making the breach not just one of the largest in terms of the number of individuals affected, but also in terms of the breadth and sensitivity of PII lost. The hackers gained entry by exploiting a website application vulnerability, and were not discovered until after they had accessed dozens of sensitive databases and created over 30 different entry points into Equifax's computer systems. [192]

To date, over 240 class action lawsuits by consumers have been filed against Equifax in the U.S., including a "50-state" complaint seeking to consolidate dozens of individual suits. [193] Those suits allege a variety of common law and statutory claims, seeking monetary damages, injunctive relief, and other related relief. [194] Equifax also faces municipal suits by Chicago and San Francisco generally alleging violations of state laws and local ordinances regarding protection of personal data, consumer fraud, business practices, and breach notice requirements. [195] Additionally, the Massachusetts Attorney General has filed a suit against the credit reporting agency in relation to the data breach. [196] Financial institutions including banks and credit unions also filed suit, seeking monetary relief for data breach costs to the financial institutions, such as canceling and reissuing credit cards and

absorbing the cost of any fraudulent charges. [197] Shareholders have also sued Equifax, alleging violations of securities laws and seeking damages against the company and its top officers. [198]

Equifax moved to consolidate the lawsuits it faces, which continue to proliferate. [199] As a result, a Judicial Panel on Multidistrict Litigation ordered centralization of the cases on December 6, 2017. [200] Going forward, litigation will be heard in the Northern District of Georgia.

Equifax was not the only bureau to have sensitive information left vulnerable. On December 20, 2017, security firm UpGuard announced that it had discovered a cache of materials on an unsecured server, this time maintained by Alteryx, a data analytics company that is partnered with the major credit bureau Experian. [201] Sensitive personal information on 123 million U.S. households was left unsecured, including datasets from Experian and the U.S. Census Bureau. [202] The exposed data included home addresses, contact information, purchasing behavior, and financial information. [203] At least two lawsuits have already been filed against Alteryx, in California and Oregon. [204]

ii. Political Breaches

The U.S. government continued investigating the July 2016 cyberattack on the Democratic National Committee, with related lawsuits drawing attention throughout 2017. Such suits included a complaint under the Freedom of Information Act filed by the Electronic Privacy Information Center against the FBI, seeking records relating to its investigation into the attack, [205] and lawsuits brought by Microsoft against command-and-control servers used by KGB hacking group "Fancy Bear" to covertly direct malware onto victims' computers. [206]

Then, on June 19, 2017, UpGuard announced that they had discovered that Deep Root Analytics, LLC, a data analytics company contracted by the Republican National Committee to gather voting data, had stored information on more than 198 million Americans on an unsecured storage server. [207] This information included names, birth dates, addresses, voter registration details, and social media posts. [208] While it is unclear whether any nefarious parties accessed the data, the breach did lead to a class action lawsuit against Deep Root. [209] That lawsuit was dismissed by the plaintiffs with prejudice in November. [210]

Additionally, the U.S. Department of Homeland Security announced in September 2017 that it appeared Russia had undertaken extensive efforts to hack state election systems in the lead-up to the presidential election. [211] Illinois had its systems breached, while 20 other states were targeted but are not believed to have been breached. [212]

iii. Customer Information

Fast Food Restaurant Chains . 2017 was a particularly notable year for data breaches at American fast food restaurants. In February, Arby's Restaurant Group Inc. revealed a breach of customer data from malicious software accessing point-of-sale systems at its restaurants; suits sprang up almost immediately. [213] In April, Chipotle Mexican Grill, Inc. announced that it had detected a security breach in its processing and transmission of customer and employee data, leading to lawsuits from financial institutions. [214] In September, Sonic Corp. was confronted with multiple suits following a data breach

announced by a security analyst, in which millions of credit and debit card users may have had their accounts pilfered. [215] Then, in October, Pizza Hut Inc. announced that it had discovered what it deemed to be a "temporary security intrusion" that compromised the PII of nearly 60,000 customers who completed orders on its website or mobile app between October 1 and 2, 2017. [216] On November 7, 2017, a class action suit was filed against the company in Washington. [217]

Hotel Groups . 2017 was not any kinder to hotel groups. Lawsuits were filed in July against Sabre Hospitality Solutions, a vendor whose electronic reservation system services thousands of travel agencies and hotels, which announced that it had suffered a data breach compromising the information of customers who made reservations using the system between August 2016 and March 2017. [218] Credit card information and cardholder names were stolen. Intercontinental Hotels Group ("IHG") is facing its own class action lawsuit, after it announced a data breach that affected 12 of its properties. Malware was found on servers which processed payments made at on-site restaurants and bars during the second half of 2016. [219] The matter is currently being briefed by IHG for dismissal.

Whole Foods . Whole Foods Market Group, Inc. found itself the target of a lawsuit following its September 28, 2017 announcement that its point-of-sale systems at taprooms and full-service restaurants (but not its grocery stores) had been hacked. The suit, a class action filed by a customer, alleges negligence on the part of Whole Foods for failing to protect her information, as well as violations of the Fair Credit Reporting Act and Ohio's Consumer Sales Practices Act. [220]

iv. Health Information

The number of data breaches affecting health care providers continued to rise in 2017, with over 340 incidents reported to the Department of Health and Human Services. [221] The past year did not, however, witness any massive breaches comparable to the 2015 attack on Anthem, which resulted in the disclosure of more than 78 million patients' PII. [222] Interestingly, of the five largest health care-related breaches in 2017, only one has resulted in litigation so far.

Commonwealth Health Corporation . In March 2017, Commonwealth Health Corporation's Kentucky-based Med Center Health announced that up to 697,800 individuals may have had their billing and health information stolen via a breach that occurred in 2014-15. [223] No hacking was involved with the breach; rather, a former employee accessed the information without authorization. This is believed to be the largest breach of a health care provider in 2017, in terms of number of records compromised. [224] While federal investigators look into the matter, at least one lawsuit has been filed against the company by affected patients. [225]

v. Law Firms and Business Information

Cyberattacks affected two large international law firms, amongst others, in 2017. While DLA Piper suffered a ransom- or wiper-ware attack that disabled the firm's communications systems for several days, no lawsuits have been filed by its clients as yet. [226] Litigation followed a data breach at the Cayman Islands-based law firm Appleby; however, it was Appleby going on the attack, suing the BBC and The Guardian over their reporting of offshore transactions by the firm's clients. [227] Millions of documents, dubbed the "Paradise Papers" by the media, were leaked to journalists detailing the

arrangements and offshore activities of Appleby's clients. [228] Appleby sued the two media companies in British court in order to force the disclosure of the documents that formed the basis of their investigation. [229]

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

While many prior data breach cases headed for settlement instead of being decided by the courts (as discussed in detail in the Settlements section below), some cases received significant rulings in the past year. Others continue to be litigated.

i. District Court Litigation

Yahoo. On August 30, 2017, a district court in the Northern District of California granted in part and denied in part Yahoo's motion to dismiss data breach litigation, opening the way for class action lawsuits to proceed against the web portal, now owned by Verizon Communications. [230] The district court ruled that some of the named plaintiffs had alleged Article III standing at the pleading stage, because they had "alleged a risk of future identity theft, in addition to loss of value of their [personal identification information]." [231] The court dismissed certain claims in the consolidated actions, but allowed the actions to continue and the plaintiffs to amend their complaints. [232]

Office of Personnel Management . The District Court for the District of Columbia dismissed a class action data breach suit stemming from the attack against the Office of Personnel Management, which compromised the personal data of current, former, and prospective U.S. government employees. [233] The court ruled that the theft of data alone was not enough to establish standing for the class and that they must allege unreimbursed out-of-pocket expenses from the alleged identity theft to state an injury in fact. [234] While the court held that two plaintiffs had alleged such expenses, it found that their claims were insufficient to establish standing because they had not sufficiently tied those injuries to the breach. [235] The court also dismissed the case on sovereign immunity and contractor immunity grounds, and found that the complaint failed to state a claim under the Privacy Act, the Little Tucker Act, and the Constitution. [236] Gibson Dunn represented OPM's co-defendant, contractor KeyPoint Government Solutions, in this litigation.

VTech . The litigation arising from a 2015 cyberattack on digital learning toy-maker VTech's servers continued to wind its way through the Northern District of Illinois. VTech won its motion to dismiss the cases against it on July 5, 2017, as the court ruled that the plaintiffs had failed to show how the data breach could lead to future harm. [237] Specifically, the court held that plaintiffs did not explain how the stolen data would be used to perpetrate identity theft. [238] However, the court did not dismiss the claims with prejudice; accordingly, plaintiffs' counsel brought an amended complaint against the company in August. [239] The case settled in early 2018. [240]

Uber. Uber won its motion to dismiss a lawsuit stemming from a 2014 data breach. The court held that the plaintiffs did not "plausibly allege an immediate, credible risk of harm" and thus lacked standing. [241] In particular, the named plaintiff did not allege that any passwords, PINs, or Social Security numbers were among the data obtained. [242] Gibson Dunn represents Uber in this dispute, which is ongoing following Plaintiffs' filing of a Third Amended Complaint.

Noodles & Co. Noodles & Co. won its motion to dismiss a proposed class action brought by financial institutions over its data breach suffered in early 2016. [243] The court found that the chain had no obligation towards the credit unions that had brought the suit. [244] The court ruled that the claims were barred under the economic loss rule. [245] Because the duties allegedly breached were contained in a network of interrelated contracts, the rule applied; because the rule only allows for recovery of damages on a breach of contract claim, the negligence claims brought by the credit unions were invalid.

ii. Appellate Litigation

CareFirst BlueCross BlueShield . The D.C. Circuit Court revived a class action lawsuit brought by policyholders of CareFirst BlueCross BlueShield health insurance, which suffered a cyberattack in 2014 leading to the theft of 1.1 million members' personal information, including names, birthdates, addresses, and subscriber ID numbers. [246] The circuit court found that the breach likely exposed Social Security and credit card numbers and other personal data such that fraudulent medical claims could result, resulting in harm concrete enough to establish standing under the Supreme Court's *Spokeo* decision. [247] Although the district court had dismissed the complaint, finding that it was based on statutory violations and not concrete harm, the appellate court found that it was plausible to infer that the hackers had the intent and ability to use the stolen data for ill, leading to concrete harm. [248]

Veterans Affairs . Conversely, the Fourth Circuit dismissed a class action suit arising from the theft of a laptop from a Veterans Affairs medical facility, which contained the unencrypted personal information of patients. [249] The circuit court agreed with the district court's ruling, finding that the plaintiffs' fear of harm from future identity theft was too speculative to confer standing, even if the plaintiffs took actions to mitigate that speculative future harm. [250] The court reasoned that the allegations of harm rested on an attenuated chain of possibilities, including the assumption that the laptop thief planned to misuse the personal information on the laptop, and planned to misuse the *plaintiffs*' personal information specifically. [251] This chain of logic was not sufficient to establish standing under *Spokeo*.

c. Trends in Data Breach Cases in 2017

Courts continued to grapple with specific issues in 2017, including issues that some had thought would be settled from Supreme Court precedent in past years, such as the *Spokeo* decision.

i. Standing Post-*Spokeo*

As seen in the appellate litigation above, the circuit courts are split when it comes to interpreting the high court's decision in *Spokeo* (and *Clapper v. Amnesty International*) regarding the tests for sufficient imminence and concrete harm to confer standing. The D.C. Circuit found in *Attias* that there was concrete harm from the CareFirst data breach, because it was plausible to infer that the hackers had the intent and ability to wrongfully use the stolen data. [252] But the Fourth Circuit found in *Beck* that there was no concrete harm from a stolen laptop containing patient information, because the harm rested on a logical chain requiring misuse of the plaintiff's specific personal information. [253] The Second Circuit used similar reasoning in *Whalen v. Michaels Stores, Inc.*, finding that a data breach leading to stolen credit card information was not sufficient to allege concrete harm, because the plaintiff had

promptly canceled her card and there were no specifics alleged regarding any other particularized or concrete injury. [254]

Like the D.C. Circuit, the Seventh, Third, and Sixth Circuits have found that risk of identity theft or credit card fraud was enough to grant constitutional standing to those who had been hacked. [255]

The Eight Circuit added a new split in September in reviving a class action lawsuit brought against SuperValu Inc., by reasoning that while there was not sufficient personal information lost to allow plaintiffs to rely on risk of imminent harm due to stolen identities, there was standing because someone had used a plaintiff's credit card to make an unauthorized purchase. [256] That allegation was sufficient to meet the concrete injury test, even though SuperValu's attorneys argued that there was no indication the purchase was a result of the breach. [257]

ii. Companies on the Attack

2017 has seen an uptick in firms taking the offensive in wielding litigation as a tool to fight hackers. For instance, Microsoft has focused its attention on the command-and-control servers used by one of the most sophisticated hacking collectives attempting to direct malware onto victims' computers. To do so, it sued Fancy Bear in the Eastern District of Virginia. [258] Microsoft argued that it had standing to sue because Fancy Bear had been using domain names that contained the names of Microsoft's products to setup websites containing malware. [259] Thereafter, Microsoft won orders from the court to compel domain name registrars to alter domains to point to Microsoft, instead of to Fancy Bear's sites. [260] Microsoft is now seeking a permanent injunction to give Microsoft ownership of the domains it has targeted. [261]

In a different vein, as noted above, Appleby has wielded litigation against journalists who reported on the Paradise Papers. [262]

Ultimately, these actions point to the possibility that other companies will take the fight to hackers, especially companies in the tech industry whose products are often targeted in order to foster data breaches.

2. Settlement Trends

As in 2016, companies facing major data breach litigation in 2017 have continued to choose to settle claims on a class-wide basis. As discussed more fully below, Anthem Inc., one of the nation's largest health insurance providers, agreed to settle a class action lawsuit brought by consumers stemming from a 2015 data security breach for $115 million. [263] Given the financial, regulatory, and reputational risks attendant to data breach litigation, this trend is understandable. Other trends emerged in 2017 as well. First, defendants in data breach litigation are continuing to settle with financial institution-plaintiffs in addition to consumer-plaintiffs. Additionally, in the aftermath of data breach settlements, some class members have objected to various elements of the settlements or proceedings. Lastly, as is discussed more fully below, defendants facing data breach enforcement have increasingly entered into settlement agreements with state attorneys general.

a. Anthem's Settlement

In 2015, Anthem, one of the nation's largest health insurance providers, announced that it had been the victim of a data breach in which hackers gained access to individuals' personal information. [264] Customer-plaintiffs brought numerous class action lawsuits against Anthem and its affiliates that were ultimately consolidated in the Northern District of California. [265] After the court denied the defendants' motion to dismiss in part, [266] the parties entered into a settlement on May 31, 2017. [267] The court preliminarily approved the settlement at the end of August. [268]

The broad strokes of the Anthem settlement are familiar. As part of the settlement, the defendants agreed to make a $115 million payment into a settlement fund. [269] The fund will be used, in part, to cover reimbursement for out-of-pocket costs and credit monitoring services for class members, [270] and to pay up to $37.95 million in attorneys' fees. [271] In addition, the defendants agreed to implement improved data security practices for at least three years and to engage an independent consultant to ensure that these practices are followed. [272]

b. Home Depot Settles with Financial Institutions

Following a 2014 data breach, in 2016 Home Depot settled a class action lawsuit brought on behalf of over 50 million of its customers for $13 million. [273] However, the settlement did not include coexisting claims brought by a consolidated class of financial institutions claiming that they were harmed by Home Depot's failure to prevent the data breach because they were required to issue consumers new credit cards and to reimburse any fraudulent charges stemming from the data breach. [274] In early 2017 Home Depot entered into an additional settlement with the financial intuitions and agreed to pay $25 million into a settlement fund intended for distribution among the class members. [275] In September 2017, the Northern District of Georgia approved this settlement. [276]

c. Developments Regarding the Target Settlement

In 2015, Target agreed to settle a consumer class action arising out of a 2013 data breach for $10 million. [277] The ultimate disposition of the case and distribution of the settlement fund, however, have been significantly delayed due to various claims by objectors. [278] For instance, in May 2017, the District of Minnesota rejected an objector's claim that the class representatives in the case had a conflict of interest with other class members such that the settlement was inadequate. [279] As of this writing, the objector's appeal is pending before the Eighth Circuit Court of Appeals. [280]

In addition, in May 2017 Target agreed to pay $18.5 million to 47 states and the District of Columbia as part of a settlement that arose out of a multi-state investigation into the same breach. [281]

d. Historical Context for Settlements of Data Breach Claims

As demonstrated in the chart below, the data breach settlements in 2017 appear to be similar to those of recent years.

Defendant	Approval	Data Type	Relief to the Class	Service Awards, Fees, & Costs
Home Depot (Financial Institution Class) [282]	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
Anthem [283]	August 25, 2017 (preliminary approval)	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 Depot (Consumer Class) [284]	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
Target Corp. (Financial Institution Class) [285]	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 [286]	$20,000 for 5 representative plaintiffs; $2.109 million in costs; $17.8 million in fees
Sony Pictures Entertainment, Inc. [287]	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

Defendant	Approval	Data Type	Relief to the Class	Service Awards, Fees, & Costs
St. Joseph Health System [288]	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
Target Corp. (Consumer Class) [289]	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
LinkedIn [290]	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
Adobe Systems, Inc. [291]	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
Sony Gaming Networks [292]	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

3. Shareholder Derivative Suits

In recent years, shareholders have occasionally responded to data breaches by filing derivative lawsuits against corporate directors and officers for breach of fiduciary duty in overseeing corporate cybersecurity. From 2014 to 2017, shareholders brought five such high-profile derivative lawsuits on behalf of Wyndham Worldwide, Target, Home Depot, Wendy's, and Yahoo. However, these suits have generally struggled to move past the motion-to-dismiss stage. Both the *Wyndham* and *Target* lawsuits

were dismissed after courts respectively found that the Wyndham board's actions were protected under the business judgment rule, [293] and that pursuing legal action against Target's directors and officers was not in the corporation's best interest. [294] The *Home Depot* case was similarly dismissed in 2015; however, the parties reached a settlement this year after the plaintiffs filed an appeal of the dismissal. The outcomes of the *Wendy's* and *Yahoo* litigations remain to be seen.

The Home Depot . After news broke that hackers stole the email addresses and credit card information of more than 50 million Home Depot customers, a number of the company's shareholders filed a derivative lawsuit in September 2015 in the Northern District of Georgia, alleging that the board of directors breached its fiduciary duty by disbanding Home Depot's infrastructure committee and moving too slowly in addressing the security breach. On November 30, 2016, the district court dismissed the action on grounds that the shareholders failed to either demand that the board take action or demonstrate with particularized facts that such a demand would have been futile. [295] Plaintiffs subsequently filed an appeal in the Eleventh Circuit. However, on April 28, 2017, the parties reached a settlement pursuant to which Home Depot agreed to adopt certain cybersecurity-related corporate governance reforms and to pay the plaintiffs' legal fees, totaling around $1.1 million. [296] The promised reforms included maintaining an executive committee on data security, documenting the responsibilities of the company's corporate information security officer, and requiring regular reports on the company's IT and cybersecurity budget. [297]

Wendy's . On December 16, 2016, just two weeks after the district court's dismissal of the *Home Depot* suit, plaintiff shareholders filed a derivative action in the Southern District of Ohio against The Wendy's Co. ("Wendy's") and certain of the company's directors and officers. The lawsuit stemmed from a data breach that occurred between October 2015 and June 2016, which affected 1,025 Wendy's franchises and spawned a series of consumer protection lawsuits. [298] The complaint asserted claims for breach of fiduciary duty, waste of corporate assets, unjust enrichment, and gross mismanagement. [299] The plaintiffs sought money damages, corporate governance reforms, and restitution of benefits and compensation. In an attempt to avoid the fate of the *Home Depot* shareholder litigation, the Wendy's plaintiffs provide detailed allegations to support their claim of demand futility, arguing that the controlling shareholder defendants have familial or past business ties with certain directors, resulting in these directors being "beholden to the controlling shareholder defendants." [300] On March 10, 2017, the Wendy's board responded with a motion to dismiss, arguing failure to state a claim and failure to make a demand or adequately plead demand futility. [301] The board members contended that the complaint was nothing more than speculation and failed to include any specific allegations that they breached any corporate duty in regard to data security protocols. [302] At the time of this writing, the board's motion to dismiss was still pending.

Yahoo . The Yahoo data breach has given rise to two shareholder derivative suits. On February 16, 2017, a Yahoo shareholder filed a lawsuit on behalf of the company in the Northern District of California. [303] On February 23, 2017, another group of Yahoo Inc. shareholders filed a second derivative lawsuit in Delaware Chancery Court. [304] Both cases have since been stayed, the former pending the entry of final judgments in the securities and consumer class actions also filed against Yahoo in the wake of the breach. [305]

C. Interceptions and Eavesdropping

1. Email Scanning

As in past years, 2017 saw key developments in class action lawsuits alleging technology companies violated state and federal laws by scanning user emails for targeted advertising and other business purposes. Companies operating electronic communications services should continue to monitor such lawsuits, as they allege privacy violations based on what many consider to be standard industry practices, concern potentially massive proposed classes including all or many users of such services, and analyze the disclosures that satisfy consent to information collection and use.

Matera v. Google Inc. Plaintiffs in *Matera v. Google Inc.* filed a class action against Google in September 2015, alleging that Gmail violates the CIPA and ECPA by intercepting emails of non-Gmail users in order to provide targeted advertising. In 2016, the court denied Google's motion to dismiss as to the merits of plaintiffs' claims, [306] and granted in part and denied in part Google's motion to dismiss based on lack of standing. [307] Most significantly, the court concluded that based on "the historical practice of courts recognizing that the unauthorized interception of communication constitutes cognizable injury" and "the judgment of Congress and the California Legislature [that] alleged violations of . . . the Wiretap Act and CIPA constitute injury in fact," the plaintiffs' complaint survived *Spokeo*. [308] However, the court also held that plaintiffs lacked standing to enjoin Google from engaging in the alleged "intercepting and scanning," which Google confirmed it had ceased. [309]

In November 2016, the parties requested a stay of the proceedings and announced that they had successfully mediated a resolution of the case and finalized a settlement agreement. [310] In a preliminary approval hearing held on March 9, 2017, the parties explained that, pursuant to the agreement, Google would be enjoined from "scanning in transit email for the *sole* purpose of collecting advertising data." [311] However, Google would be allowed to scan incoming in-transit email for "the 'dual purpose' of (1) detecting spam and malware and (2) obtaining information that would be 'later used for advertising.'" [312] Google also agreed to pay $2.2 million in attorneys' fees, $2,000 for each of the two lead plaintiffs, and $123,500 for the settlement administrator. [313]

On March 15, 2017, the court rejected this settlement offer, stating that the class settlement notice was "inadequate" because it was "difficult to understand." [314] In particular, the preliminary settlement failed to clearly disclose the "dual purpose" to which Google agreed or "the fact that Google intercepts, scans, and analyzes the content of emails sent by non-Gmail users to Gmail users for the purpose of creating user profiles" for targeted advertising. [315] Furthermore, the court found that it was not clear whether the changes Google planned to make would bring Google into compliance with the CIPA and ECPA. [316]

On July 21, 2017, the parties proposed a new settlement, which included a "plain language" recap of the changes Google plans to make. [317] The summary stated that for three years, Google would "cease all automated scanning of emails sent to Google accounts for advertising purposes while the emails are in transmission prior to delivery to the Gmail user's inbox." The settlement does not prohibit Google from scanning email for the prevention of spam or malware. In addition, Google stated that it is making

"business-related" changes to Gmail, whereby it "will no longer scan the contents of emails sent to Gmail accounts for advertising services," either during the transmission process or after the emails have been delivered. These changes are not subject to the three-year time period, and are independent of the settlement. [318] The court preliminarily approved the revised settlement on August 31, 2017. [319] A final fairness hearing is scheduled for February 8, 2018.

Cooper v. Slice Technologies, Inc. & UnrollMe Inc. In *Cooper v. Slice*, plaintiffs brought a class action for damages and injunctive relief, alleging that UnrollMe and its parent company, Slice Technologies, violated the ECPA and SCA by failing to adequately disclose UnrollMe's practice of scanning emails and selling data to third parties. [320] UnrollMe is a web service that unsubscribes users from mailing lists, newsletters, and other unwanted emails. [321] Plaintiffs asserted that UnrollMe intercepted and accessed user's emails without consent or authorization, or exceeded authorization by accessing emails for the purpose of extracting and selling consumer data. [322]

Defendants moved to dismiss the lawsuit on October 12, 2017. [323] Among other things, defendants argued that plaintiffs failed to allege injury in fact to establish Article III standing under *Spokeo*, since plaintiffs did not allege their actual emails were sold to other companies, or that anonymized data that was extracted from plaintiffs' emails was reidentified after being sold. Defendants also asserted that plaintiffs failed to state a claim under the Wiretap Act because defendants purportedly disclosed the activities at issue in their privacy policy, and because plaintiffs alleged only access to their stored emails, whereas the Wiretap Act applies to the "interception" of communications.

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. [324] The vast majority of states have similarly adopted a "one-party" consent requirement. [325] A minority of states have arguably adopted either a "two-party" or "all-party" consent requirement. [326]

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, much of the litigation surrounding unauthorized recordings has arisen out of California's Invasion of Privacy Act ("CIPA"), California Penal Code § 630, *et seq*. [327] Most call recording litigation based on CIPA has focused on §§ 632 and 632.7, which prohibit eavesdropping on calls to landlines and cell phones, respectively.

Recently, courts have held that non-California plaintiffs may assert CIPA claims against California defendants where the alleged violations occurred in California. [328] Indicative of this national reach, California business owners brought suit in Illinois against various banks and telemarketers alleging illegal recordings of discussions containing sensitive business information. [329] The various defendants filed motions to dismiss, transfer, and sever the case, but the case is still pending in the Northern District of Illinois. Significantly, some of the defendants have sought to change venue based

on forum selection clauses in their customer or user agreements, rather than challenging the ability of plaintiffs to bring CIPA claims outside of California, indicating that few litigants are willing to challenge the national reach of CIPA.

Also in the realm of jurisdictional issues related to CIPA, the Ninth Circuit recently reversed a decision to remand a CIPA class action back to state court, concluding that the plaintiff had failed to demonstrate that two-thirds of the class actually resided in California, as required by the Class Action Fairness Act ("CAFA"). [330] Specifically, CAFA exempts from federal jurisdiction "home-state controversies," where at least two-thirds of the proposed class and the primary defendants are all citizens of the State in which the action was originally filed. [331] Plaintiffs' proof that two-thirds of all class members were Californians was lacking, according to the Ninth Circuit, because, although the class contained an indeterminate number of people who were "located in" California when they received the allegedly improperly recorded phone calls, the allegations never specified how many of them were California citizens or even how large the whole class was. [332] In reaching its decision, the court noted that Plaintiffs were aware of the class definition issue and failed to carry their burden of proving the citizenship of a sufficient number of class members. [333]

In the class certification context, in *Raffin v. Medicredit, Inc.*, the Central District of California certified a CIPA class action against Medicredit, a debt collector, for recording cell phone calls and failing to inform plaintiffs of the recording. [334] The action sought certification of a § 632.7 class, which prohibits the recording of cell phone communications. [335] Notably, the court concluded that the class was ascertainable for certification purposes, even though it may be necessary to undertake the challenging process of using cell site location information to verify that putative class members were in California when called. [336] In analyzing § 632.7 more generally, the court also concluded that a party must be informed "at the outset," meaning "prior to *any* recording of the plaintiff's communication," that the call is being recorded. [337] Subsequent courts have adopted this interpretation of § 632.7, suggesting a broadening of the law's scope. [338]

If this becomes settled law, it would align the law under § 632.7 with that under § 632, which already requires notification "at the outset" for any recordings of calls over a landline. However, class certification appears to be more difficult under § 632 than § 632.7, as the more generous test applied in *Raffin* diverges from the stricter analysis in *Saulsberry v. Meridian Financial Services, Inc.*, decided last year. [339] This may be an indicator of a unique area of divergence in the interpretation of two statutes that are otherwise converging, or it may represent a reversal of the trend of denying class certification. Ultimately, very few §§ 632 and 632.7 class certification cases have been decided this year, but all three have granted class certification. [340]

Adding to the body of law regarding the scope of § 632.7, the court in *Ronquillo-Griffin* concluded that § 632.7, like § 632, applies to parties to a communication, not just third parties, adding to the already significant number of district courts who have so interpreted § 632.7. [341] Like the *Raffin* case discussed above, this indicates an increasing overlap between § 632 and § 632.7, generating a more consistent body of law between call recordings over landlines and cell phones.

On the criminal side, the California Court of Appeal invalidated part of CIPA. [342] California Penal Code § 632(d) renders inadmissible as evidence recordings obtained without all parties' consent. However, California's constitution contains a "Right to Truth-in-Evidence" provision, which permits all relevant evidence to be admitted unless the legislature provides otherwise by a two-thirds majority vote. [343] The Court of Appeal concluded that this provision abrogated the inadmissibility component of CIPA, rendering recordings that otherwise violate CIPA admissible. [344]

Outside of California, there has also been some litigation regarding the scope of local eavesdropping statutes. The Arizona Court of Appeals confirmed that a phone message may be shared by the recipient of the message, even if the person leaving the message does not consent. [345] In *State v. Smith*, the defendant had argued that, when leaving a voice message, there is only one "participant," to the call, but the court rejected this logic, concluding that the recipient of the message is also a participant and may consent to sharing the recorded voicemail. [346] In a similar case—also captioned *State v. Smith* —the Supreme Court of Washington considered whether an inadvertent recording through the voicemail function of a cell phone falls within the purview of Washington's all-party consent statute. [347] The Court concluded that "the plain language of the act confirms that even an inadvertent recording of a private conversation falls within the purview of the act." [348]

3. Other "Interceptions"

Emails and telephone calls are not the only communications that can be intercepted, and plaintiffs are increasingly bringing lawsuits based on novel theories of interception and collection of data. This year saw a number of developments in ongoing lawsuits, as well as several actions alleging new theories of Wiretap Act violations.

Opperman et al v. Kong Technologies, Inc. et al. In April 2017, several major tech companies, including Twitter, Yelp, Instagram, Foursquare, and Path, agreed to settle a putative class action accusing them of violating the ECPA and the Texas Wiretap Act, among other common law privacy rights. [349] The putative class action complaint, originally filed in 2012, alleged that the defendants' applications access user contact information without their consent. [350] For instance, plaintiffs claimed that Twitter's "Find Friends" feature violated consumer privacy by scanning users' address books to see which of their contacts are on Twitter. Twitter, on the other hand, argued users were informed of the process and gave their permission for the service to scan their address books. Path users alleged that the photo sharing and messaging app was accessing their contacts and calendar information without permission. Path later issued an apology. Plaintiffs agreed to pay a consolidated $5.3 million as part of a deal, which covers a proposed class of an estimated 7 million claimants who downloaded the companies' iOS apps on their Apple devices and activated the "Add Friends," "Find Friends" or "Suggested Friends" feature offered by the relevant application. [351] A final approval hearing was held on December 14, 2017.

In re Vizio, Inc., Consumer Privacy Litig **.** In this putative class action complaint, plaintiffs alleged that Vizio violated the ECPA and the VPPA, as well as several state law fraud, negligent misrepresentation, and consumer protection claims, by using their smart TVs to secretly collect, and distribute to advertisers, information on customer viewing habits so that advertisers could deliver

targeted advertising in real time. [352] On March 2, 2017, the court granted Vizio's motion to dismiss plaintiffs' Wiretap Act, state law video privacy, negligent misrepresentation, affirmative fraud, and California false advertising claims with leave to amend. Vizio's motion was denied as to plaintiffs' VPPA, fraudulent omission, state privacy law, and unjust enrichment claims. With respect to the Wiretap Act claims, the court found that plaintiffs failed to adequately plead simultaneous interception (relying instead on vague allegations about how Vizio's data collection occurred in "real time"), but did not reach Vizio's argument that its collection and disclosure software does not capture the "contents" of electronic communication. [353] On March 23, 2017, plaintiffs filed a second consolidated complaint that dropped all of the dismissed causes of action except the Wiretap Act claims. [354] Addressing the deficiencies in the prior complaint, plaintiffs now alleged that Vizio's software takes samples of the programming displayed on a TV at any point in time and sends fingerprints of those samples to the centralized fingerprint 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." [355]

On April 13, 2017, Vizio moved to dismiss plaintiffs' Wiretap Act claims for failure to state a claim, attacking only whether its software captures the "contents" of electronic communications. [356] Denying dismissal on July 25, 2017, the court ruled that because the intended message conveyed by Vizio's software communication is the program being watched, the intercepted data extends beyond metadata to samples of the actual content. [357] The court also dismissed Vizio's assertion that its software does not collect the contents of electronic communications because the samples are "tiny" and "unrecognizable," noting that the standard for determining whether information qualifies as content data does not depend on how much content is collected or whether the intercepted information would be "recognizable." [358]

In its motion to dismiss, Vizio also argued that plaintiffs' demand for injunctive relief was moot because a recent agreement with the FTC and New Jersey Attorney General—in which Vizio was fined $2.2 million and agreed to obtain affirmative express consent before collecting any consumer data—ensured the offensive data collection had stopped. [359] Finding that the agreements were insufficient to ensure that Vizio's improper data collection would not recur, the court denied Vizio's motion to dismiss on mootness grounds. [360]

Satchell v. Sonic Notify, Inc. In a class action filed in August 2016, plaintiff alleged that the Golden State Warriors' mobile app, developed by YinzCam, uses the phone's microphone to track users' locations by picking up on sonic beacons built by Signal360, and violates the Wiretap Act by secretly recording users' conversations in the process. [361] Defendants moved to dismiss on November 1, 2016, and on February 13, 2017, the court granted the motion in part and denied it in part. [362] The court ruled that although plaintiff alleged sufficient facts to demonstrate she suffered an injury in fact from the purported spying, she did not sufficiently allege a violation of the Wiretap Act because she failed to show how the defendants intercepted and then used those oral communications. [363] Plaintiff filed an amended complaint on March 13, 2017, [364] in which the court determined she cured those defects by alleging sufficient facts to show defendants intercepted an oral communication. [365] In a November 20, 2017 decision denying defendants' motion to dismiss, the court explained, "Plaintiff cites at least four instances where she had her phone with her, the app was running and she had conversations about private matters,

including nonpublic information during a business meeting and private financial matters." [366] However, the court dismissed YinzCam from the lawsuit, ruling that plaintiff failed to demonstrate that the company was more than a conduit for the alleged communications that were intercepted by the Warriors and Signal 360. [367]

Rackemann v. Lisnr, Inc. et al. In October 2016, the NFL's Indianapolis Colts, and audio software companies involved in creating the Colt's mobile app, faced similar allegations that beacon technology was used to spy on the conversations of fans using the teams' app. [368] Defendants moved to dismiss, and on September 29, 2017, the court denied defendants' motion with respect to plaintiff's interception claims and granted it with respect to their use claims. Regarding interception, the court rejected defendants' argument that plaintiff need allege specific details of communications that may have been intercepted, finding that it was reasonable to infer that plaintiff's smartphone was activated while he was engaged in a private conversation over a four-year period. [369] The court also found that plaintiff adequately plead that his communications were captured and the content acquired, as he asserted that the app recorded portions of audio, including private conversations, captured by the phone's microphone, and that audio was analyzed by defendants. [370] Following the Sixth Circuit's recent decision in *Luis v. Zang*, the court refused to dismiss Adept Mobile, the audio software company that, among other things, maintained the code for the app and integrated the audio technology into the app. [371] Citing the Sixth Circuit, the court explained that "allegations of defendants working in concert or participating in the interception of communications can suffice to state a claim." [372] The court did, however, dismiss plaintiff's claim that defendants "used" intercepted data, as plaintiff pled no facts showing that the contents of plaintiff's communications, as opposed to beacon signals, were used to send targeted advertising. [373]

Zak v. Bose Corp. In a putative class action, plaintiff accused Bose of violating the Wiretap Act and the Illinois Eavesdropping Statute by secretly collecting, transmitting, and disclosing the private music selections of customers who downloaded Bose's mobile app. [374] Bose's app allows users to pair their mobile devices with Bose wireless headphones and access key features, such as controlling the content they play. [375] Plaintiff asserted that when he used the Bose app to view information about and control music playing on his Bose headphones, Bose collected and retained the song information displayed in the app. [376] Plaintiff alleged that this collection constitutes an interception of electronic communications between Bose users and streaming music providers such as Spotify. [377]

In a motion to dismiss filed on August 3, 2017, Bose argued that the Wiretap Act does not apply to Bluetooth communications between an app and headphones because such communications operate between devices in close physical proximity, and do not effect interstate or foreign commerce. [378] Furthermore, Bose contended that the Wiretap Act and the Eavesdropping Statute do not apply to communications where the interceptor is one of the parties, and the communications at issue occurred between plaintiff's Bose headphones and Bose's app. [379]

Allen v. Quicken Loans Inc. and Navistone, Inc. In December 2017, Quicken Loans was hit with a proposed class action alleging it breached the Wiretap Act by installing software on its website that secretly tracks visitors' keystrokes, mouse clicks, and other electronic communications in order to gather personally identifiable information and de-anonymize their names and addresses. [380] This action,

which was filed in the District of New Jersey, follows two nearly identical lawsuits brought by the same plaintiff's firm against mattress seller Casper and retailer Moosejaw. [381]

D. Telephone Consumer Protection Act

The past year has been eventful for actions under the TCPA. [382]

Perhaps the most anticipated TCPA topic in 2017—the D.C. Circuit's ruling in *ACA International v. FCC*—remains outstanding. [383] *ACA International* interprets the FCC's 2015 omnibus Declaratory Ruling and Order (the "omnibus order") that, among other things, defined an autodialer to include any equipment with the "potential ability" to store or produce telephone numbers to be called or to call those numbers, as opposed to equipment with the *current capability* to do this. [384] The omnibus order also changed the means through which a consumer can revoke consent. Under the omnibus order, not only may "a called party . . . revoke consent at any time and through any reasonable means," but "[a] caller may not limit the manner in which revocation [of consent] may occur." [385] Oral argument was held in October 2016 and lasted for over two hours, but the D.C. Circuit has yet to issue a decision.

In Congress, both sides of the aisle appeared interested in amending the TCPA. In late 2016, the House Energy and Commerce Committee's Subcommittee on Communications and Technology held a hearing on the TCPA wherein a Democratic ranking member applauded a move to modernize the TCPA, [386] and the Republican subcommittee chairman stated "it is increasingly clear that the law is outdated and in many cases, counterproductive." [387] Though Congress has not yet acted, some of Congress's possible changes to the TCPA could be to cap statutory damages at $500,000 (matching the Truth in Lending Act's cap) [388] or to update the TCPA to reflect the increased use of text messaging and the creation of apps that could turn a smartphone into an autodialer.

Yet Democrats and Republicans have not agreed on every TCPA issue in 2017. For example, in March 2017, the FCC received a petition from All About the Message LLC seeking a declaration that the use of ringless robocalls that go straight to voicemail do not violate the TCPA. [389] After the FCC issued a request for public comment, eleven Democratic Senators sent a letter to the FCC urging it to protect consumers from such calls, while the Republican National Committee voiced support for the petition. [390]

Even though Congress did not pass legislation amending the act, FCC leadership changed in 2017. The FCC, which has interpretative authority over the TCPA, is statutorily required to have two commissioners from each party, and, for the past several years, was led by three Democrats and two Republicans. [391] Following the inauguration of President Trump, the FCC now has three Republicans and two Democrats. [392] In the upcoming year, it is likely that the Republican commissioners will scale back FCC enforcement of the TCPA. [393] Commissioner Michael O'Reilly, a Republican, vehemently disagreed with the FCC's 2015 omnibus order, and Chairman Ajit Pai applauded the D.C. Circuit's March ruling in *Yaakov v. FCC*, which held that the FCC lacked the authority under the TCPA to require opt-out notices on solicited faxes. [394] Chairman Pai previously has been critical of plaintiff's counsel's choice of litigation targets, noting that these "lawyers have found legitimate, domestic businesses a much more profitable target" for TCPA litigation, rather than "go[ing] after the

illegal telemarketers, the over-the-phone scam artists, and the foreign fraudsters." [395] The sentiment of the current leadership suggests some regulatory restraint in 2018.

The past year also saw the resolution of several closely-watched cases. In *Krakauer v. Dish Network LLC*, a jury awarded damages to a class of plaintiffs who allegedly received unwanted phone calls. [396] The court ordered treble damages on the basis that Dish allegedly had knowledge that its marketing firm had repeatedly violated the TCPA. [397]

In *United States v. Dish Network LLC*, the district court found that Dish Network violated the TCPA and state laws through both its direct telephone marketing and third-party telephone marketing campaigns. [398] The civil penalties ordered in the case included awards to both the federal government and the state participants in the suit: California, Illinois, North Carolina, and Ohio. [399] The matter is currently on appeal. [400]

In *Birchmeier v. Caribbean Cruise Line, Inc.*, the parties agreed to a $76 million settlement of a class action accusing several cruise marketing companies of robocalling. [401] The agreement provides a minimum of $135 per call where the vast majority of class members claimed three calls, leaving plaintiffs with a much higher payment than is typical in a TCPA class action settlement of this size. [402]

E. Video Privacy Protection Act

In 2017, courts resolved some significant VPPA-related cases that had been filed in previous years. The VPPA, which was enacted in 1998 following a D.C. newspaper's disclosure of Supreme Court nominee Judge Robert Bork's video rental records, [403] prohibits "video tape service providers" from "knowingly" disclosing "personally identifiable information concerning any consumer" to third parties. [404] The VPPA was originally intended as a straightforward rule to prevent video stores from disclosing the video-rental habits of its patrons. Over 20 years later, courts continue to grapple with applying this antiquated law to constantly changing technologies.

This year, courts addressed three main issues as related to the VPPA: (1) standing, (2) the definition of "personally identifiable information," and (3) the definition of "consumer" or "subscriber." While there is an emerging consensus on the procedural issue of standing, courts remain split on how to apply the more substantive provisions of the statute.

Both circuit courts to address the issue of standing this year found that an allegation of mere disclosure in violation of the VPPA is sufficient to meet Article III's standing requirements. In *Eichenberger v. ESPN, Inc.*, plaintiffs alleged that ESPN had disclosed users' "personally identifiable information" to Adobe Analytics, a third-party analytics company, in violation of the VPPA. [405] Joining every circuit court [406] and all district courts [407] that have addressed the issue post-*Spokeo*, the three-judge panel held that the plaintiff did not need to allege any further harm beyond a disclosure of "personally identifiable information" to plead Article III standing. [408] As described above, in *Spokeo v. Robins* the Supreme Court strengthened the requirements for Article III standing, requiring allegations of a concrete injury rather than a mere statutory violation. [409] In finding that disclosure in and of itself constitutes a concrete harm, the Ninth Circuit in *Eichenberger* explained that the VPPA confers a *substantive right* to privacy, meaning that "every disclosure" of an individual's personally identifiable

information and video-viewing history "offends the interests" the VPPA protects. [410] Earlier this year, in *Perry v. Cable News Network*, the Eleventh Circuit similarly found that a disclosure alone, even without any alleged misuse of information, satisfied Article III standing requirements. [411] The precedent set by these decisions sets a low barrier for entry for plaintiffs to bring suit under the VPPA, which may yield an increase in VPPA litigation.

Circuit courts have taken different approaches in addressing the scope of "personally identifiable information," but the significance of any differences between the two tests is yet to be determined. The VPPA defines "personally identifiable information" to "include[] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." [412] As discussed in our 2016 Year-End Update , the First and Third Circuits articulated two separate tests to determine what information Congress intended to cover in this statute. In *Yershov v. Gannett*, the First Circuit diverged from virtually all district courts in embracing a broader definition of "personally identifiable information," holding that it extends beyond a person's name to include "information *reasonably and foreseeably likely* to reveal which . . . videos [a person] has obtained." [413] The court concluded that GPS coordinates and a device ID fell within this definition. [414] In contrast, in *In re Nickelodeon Consumer Privacy Litigation*, the Third Circuit adopted an "ordinary person" test, finding that "personally identifiable information" includes only information that "would readily permit an *ordinary person* to identify a specific individual's video-watching behavior." [415] In finding that digital identifiers such as MAC addresses and IP addresses did not constitute "personally identifiable information," it explained that Congress's purpose in passing the VPPA was narrowly restricted to preventing "disclosures of information that would, with little or no extra effort, permit an ordinary recipient to identify a particular person's video-watching habits." [416] In January 2017, the Supreme Court denied certiorari, [417] declining to address what some have characterized as a split between the two circuit courts.

In *Eichenberger*, Ninth Circuit considered both of these standards, but ultimately adopted the narrower "ordinary person" test promulgated by the Third Circuit. Notably, the court instructed that the statute "looks to what information a video service provider discloses, not to what the recipient of that information decides to do with it." [418] The court held that the information allegedly disclosed to Adobe by ESPN—(1) the serial number of the plaintiff's Roku device, and (2) the identity of videos the plaintiff had watched on the WatchESPN Channel application—could not be used by an "ordinary person" to identify an individual. The fact that Adobe might be able to identify the individual with other personal information in its possession, that ESPN never shared nor possessed, was irrelevant. The court reasoned that this test "fits most neatly" with congressional intent, stating that "the advent of the Internet did not change the disclosing-party focus of the statute." [419] By assessing liability based on the information disclosed from the disclosing party's perspective, companies should be able to better assess their compliance with the law. Although these courts have applied different standards, both the Third and Ninth Circuits assert that the practical differences may be minimal. [420]

On the other hand, the Central District of California applied the First Circuit standard in *In re Vizio, Inc. Consumer Privacy Litigation* . In that case, plaintiffs alleged that Vizio violated the VPPA and the ECPA by using their televisions to secretly collect, and distribute to advertisers, information on customer viewing habits. [421] In denying in part defendants' motion to dismiss, the court held that the disclosure

of "consumers' MAC addresses and information about other devices connected to the same network" could qualify as "personally identifiable information" under the VPPA because MAC addresses are "frequently linked to an individual's name and can be used to acquire highly specific geolocation data." [422] This case will be one to watch this year; the district court denied Vizio an immediate appeal of the decision to the Ninth Circuit, [423] and the next filing regarding a motion to compel was due on January 3, 2018.

The final issue considered by courts this year was the issue of who is a "subscriber," and thus a "consumer," under the statute. In *Perry v. Cable News Network*, the plaintiff alleged that CNN violated the VPPA by tracking his views of news articles and videos on the CNN app and disclosing this information to third parties. In affirming the dismissal of the putative class action, the court found that the plaintiff did not qualify as a "subscriber" because he had not established an account with CNN, provided any personal information, made any payments, become a registered user, received a CNN ID, or established a CNN profile. [424] Thus, he had not "demonstrated an ongoing commitment or relationship with CNN." [425] In *In re Vizio*, on the other hand, the court held that plaintiffs are "subscribers" based on the allegation that Vizio charges them a premium for its smart TVs because of the video content it provides. [426] Additionally, the court found that plaintiffs plausibly alleged that Vizio is a "video tape service provider" because it is engaged in the business of delivering video content. [427]

In 2017, courts sought to add more clarity to VPPA jurisprudence. With the exception of the First Circuit and Central District of California, most courts have interpreted the VPPA narrowly and relieved media companies of liability. Nevertheless, plaintiffs who can clear the *Spokeo* standing bar are likely to continue to bring suit under the VPPA in the hope of winning substantial statutory damages.

F. California's Song-Beverly Credit Card Act and Point-of-Service Data Collection

There were few cases this year arising under California's Song-Beverly Credit Card Act, which prohibits merchants from requesting and recording "personal identification information" concerning the cardholder during credit card transactions. [428] The lack of cases is likely due to the impact of the U.S. Supreme Court's decision in *Spokeo, Inc. v. Robins*, [429] which defendants have invoked to defeat class actions brought under Song-Beverly. Indeed, in the one significant case this year, *Medellin v. IKEA U.S.A. W., Inc.*, the representative plaintiff alleged that IKEA had requested and collected her ZIP code as part of her credit card purchases, but conceded that "she alleged only a bare procedural violation of the [Song-Beverly] statute and suffered no other cognizable harm" as required for standing. [430] The Ninth Circuit consequently vacated the district court's judgment and remanded the case with instructions to dismiss without prejudice for lack of standing—due to the fact that the plaintiff's claim did not "satisfy the injury-in-fact requirement of Article III." [431] IKEA appealed to the U.S. Supreme Court, seeking to expand the *Spokeo* doctrine, but the Supreme Court declined certiorari on October 2, 2017. [432]

The lack of significant Song-Beverly cases in 2017 may be explained a number of ways. It is likely that some plaintiffs decided to wait for the outcome of the Supreme Court's certiorari decision in *Medellin* before moving forward with their case. It is also likely that possible plaintiffs are exploring how best to argue that their violations of Song-Beverly satisfy Article III standing requirements, especially after the

Medellin plaintiff conceded that her allegations did not. Regardless, we can expect that after *Spokeo* and *Medellin*, many plaintiffs were forced to revise their litigation strategy to adapt to these decisions or determine whether California state courts may be a preferred venue, given that *Spokeo* has evidently narrowed federal class action doctrine. As a result, we may see new cases with novel arguments for standing brought in 2018.

G. Biometric Information Privacy Acts

In 2017, companies have continued to integrate biometric technology into both their products and their day-to-day operations. In previous years, Texas and Illinois enacted legislation regulating the collection and use of certain biometric data. In July of 2017, Washington became the third state to enact such legislation, requiring in certain circumstances that commercial entities "provid[e] notice, obtain[] consent, or provid[e] a mechanism to prevent the subsequent use" of biometric data before collecting such information. However, like Texas's law, and unlike the Illinois Biometric Information Privacy Act ("BIPA"), the Washington bill does not provide a private right of action.

The private right of action allowed by the Illinois BIPA continues to energize the plaintiff's bar, which in 2017 filed dozens of class actions against companies for their allegedly improper collection of alleged biometric information. Plaintiffs in these cases have generally fallen under one of two categories: (1) employees of companies that allegedly utilize biometric information, such as fingerprints, for time keeping purposes; and (2) customers of companies (often in the technology industry) that use alleged biometric information to enhance the consumer experience, such as photo sharing and social media services.

The first category of plaintiffs represents a relatively new trend in BIPA litigation, as 2017 witnessed a surge of class actions by employees of companies using alleged biometric timekeeping methods. For example, in October, employees of Illinois trucking company RJW Transport filed suit against the company, alleging that it captured and stored their fingerprints for timekeeping purposes, "without obtaining informed written consent or publishing its data retention and deletion policies," as required by statute. Similarly, employees of hotel chain Hyatt filed an action against their employer, claiming that they suffered "serious and irreversible privacy risks," such as risk of identity theft, as a result of the collection of their fingerprints. These suits are just two of many class actions filed in relation to alleged biometric timekeeping systems in the past year; however, these cases may come to a quick end in light of a December decision from the Illinois Second District Appellate Court in which the court held that "[i]f a person alleges only a technical violation of the Act without alleging any injury or adverse effect, then he or she is not aggrieved and may not recover under" BIPA. [433]

Consumer class actions were the second primary category of BIPA cases facing courts this year. There have been two major issues arising out of consumer-driven litigation recently: (1) Article III standing; and (2) the photograph exception of BIPA. Several court opinions in 2017 addressed these issues and will likely affect plaintiffs' litigation strategies moving forward.

First is the matter of Article III standing. Our 2016 Year-End Update described defendant's motion to dismiss in *In re Facebook Biometric Information Privacy Litigation*, a suit in which plaintiffs alleged

that Facebook's facial recognition and photo tagging system violated the Illinois BIPA. Facebook argued that plaintiffs had not suffered a concrete harm sufficient to establish Article III standing. The court stayed Facebook's motion pending the Ninth Circuit's decision on remand in *Robins v. Spokeo, Inc*. The court heard oral argument in November 2017 after that *Spokeo* decision came down, but has not yet issued a ruling.

Meanwhile, in November, the Second Circuit affirmed dismissal of the complaint in *Santana v. Take-Two Interactive Software, Inc.* on the ground that plaintiffs, consumers of a video game that used facial recognition technology to create life-like player personas, alleged harms that were merely procedural, and did not show a "risk of real harm" under *Spokeo* absent allegations that the company was misusing the collected biometric information. This decision will likely make it difficult, at least in the Second Circuit, for consumer plaintiffs to bring class actions for mere procedural violations of BIPA.

The second key issue impacting consumer class actions this year was whether BIPA covers the practice of scanning facial features from digital photographs; specifically, whether such scanning technologies are excluded from BIPA's protection of "biometric identifiers" under the statute's exception for "photographs." In 2016, in *Facebook*, the court held that this alleged conduct did not fall under the photographs exception, reasoning that the term "photographs" is listed along with other "low-tech" categories of data in the statute—such as writing samples and physical descriptions—and thus was only intended to refer to "paper prints of photographs, not digitized images."

In 2017, the Northern District of Illinois reached a similar conclusion about facial scanning technologies, but under a different analysis. In *Rivera v. Google, Inc.*, plaintiffs alleged that Google extracted biometric identifiers from digitized photographs without users' consent. Google argued in its motion to dismiss that the statute did not regulate biometric data derived from these photograph based on a plain reading of the exception. The judge rejected Google's argument, reasoning that although the photographs exception *did* excuse Google's storage of the photographs themselves, it did not cover the collection of face geometry data *derived therefrom* . Furthermore, the judge wrote, there was nothing in the text of the legislation to suggest that biometric identifiers must be derived from a person in real time. Google has since appealed the district court's decision.

H. Internet of Things and Device Hacking

The Internet of Things ("IoT") is continuously expanding as traditional devices are becoming increasingly "smart" and connected. Throughout 2017, corresponding with an increase in the IoT, there was an increase in regulatory guidance and regulatory and private actions related to smart and connected devices.

1. Connected and Autonomous Vehicles

Concerns about security breaches and privacy violations related to self-driving and other automobile software have played an important role during recent legislative developments in this area. The House passed the Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution, or SELF DRIVE, Act on September 6, 2017. [434] The bill largely allows automakers to set their own cybersecurity standards, including a plan to deal with "reasonably foreseeable vulnerabilities" in their

systems. [435] On October 4, 2017, the Senate approved its own version of the bill, the American Vision for Safer Transportation through Advancement of Revolutionary Technologies ("AV START") Act. [436] A recent amendment requires that manufacturers develop, maintain, and execute a written plan for identifying and reducing cybersecurity risks to the motor vehicle safety of automated vehicles. The Senate Commerce Committee plans to hold a hearing on self-driving and other auto technologies on January 24, 2018. [437] For further detail, please see our 2017 client alert Accelerating Progress Toward a Long-Awaited Federal Regulatory Framework for Autonomous Vehicles in the United States .

On June 28, 2017, the FTC and the National Highway Traffic Safety Administration ("NHTSA") hosted a workshop to examine the consumer privacy and security issues posed by automated and connected cars among industry representatives, consumer advocates, academics, and government officials. [438] In her opening remarks, Acting FTC Chairman Maureen Ohlhausen emphasized the potential benefits of connected cars and stressed that while the FTC would use its enforcement powers under the FTC Act, its approach would be one of "regulatory humility"—aiming to "avoid unnecessary or duplicative regulation that could slow or stop innovation." She urged Congress to consider data security and data breach notification legislation to "strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach." [439] Highlighting the importance of collaboration between industry and regulators, stakeholders also pointed to self-regulatory efforts such as the Alliance of Automobile Manufacturers' Privacy Principles for Vehicle Technologies and Services voluntary industry standards, which went into effect in January 2016. [440]

Developments continued on the litigation front as well. In July 2015, Chrysler and Harmon International Industries voluntarily recalled their vehicles because the vehicle computer system ("uConnect") had design vulnerabilities that could allow hackers to take remote control of the vehicle's functions. [441] In *Flynn v. FCA US LLC*, plaintiffs alleged that these vulnerabilities violated the Magnuson-Moss Warranty Act and Michigan, Illinois, and Missouri state laws. [442] In August 2017, the court dismissed all 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. [443] On October 13, 2017, plaintiffs asked the court to certify a class of 1.4 million car owners. [444] Automaker FCA US LLC moved for summary judgment on all plaintiffs' claims on October 5 and subsequently filed alternative motions for summary judgment against particular plaintiffs. [445] On November 6, 2017, plaintiffs opposed these motions. [446]

In November 2015, in *Cahen v. Toyota Motor Corp.*, the court granted Toyota, Ford, and General Motors' motions to dismiss a class action complaint alleging, among other claims, that the vehicles' computers were vulnerable to hacking and privacy violations related to their computer software. [447] In September 2016, plaintiffs appealed to the Ninth Circuit, arguing that the district court erred in holding that plaintiffs failed to establish standing to assert their claims. [448] On December 21, 2017, the Ninth Circuit affirmed the district court's dismissal, noting that the alleged risks and defects were speculative and that plaintiffs had not pleaded sufficient facts demonstrating how the aggregate collection and storage of non-individually identifiable driving history and vehicle performance data caused an actual injury. [449]

2. Routers, Cloud Storage, and Connected Cameras

On January 5, 2017, the FTC sued D-Link, a provider of wireless routers and IP-connected cameras, in the Northern District of California for alleged violations of the FTC Act. [450] As outlined in our 2016 Year-End Update , the FTC alleged that D-Link engaged in unfair and deceptive practices by advertising its routers and cameras as containing "Advanced Network Security," while flaws in D-Link's security allow hackers to easily access consumers' information and cameras. [451] The complaint against D-Link alleges one count of unfairness relating to D-Link's failure to secure consumer's information and five counts of misrepresentation relating to D-Link's advertising and statements that its routers and internet cameras are secure. [452] On September 19, 2017, the court dismissed the FTC's unfairness claim and two of the misrepresentation claims under Section 5 of the FTC Act. The district court ruled that, in the absence of a breach, the FTC had failed to allege that device security flaws caused or were likely to cause substantial consumer harm, and that two misrepresentation claims, which centered on alleged misrepresentations in promotional materials for IP cameras and graphic user interfaces ("GUI"s) for routers, lacked specificity as to the deceptive conduct alleged. [453] The district court allowed the remaining three misrepresentation claims to continue. [454]

3. Smart TVs

Private actions against smart television manufacturers have continued apace along with the rapid growth of consumer demand for the devices. In the most prominent case, plaintiffs alleged that Vizio violated the VPPA and the ECPA by using their televisions to secretly collect, and distribute to advertisers, information on customer viewing habits. [455] In July 2017, the court denied Vizio's motion to dismiss, finding that the agreement the company struck with the Federal Trade Commission and New Jersey's Attorney General was insufficient to ensure that Vizio's improper data collection would not recur. [456] Similarly, in March 2017, a proposed class action was filed against Samsung Electronics America Inc. and its parent company Samsung Electronics Co. Ltd., claiming that smart TV devices with the capability to respond to human voices through a built-in "always on" recording device were being used by the company to intercept and record consumers' private communications inside their homes for profit, violating the New Jersey Consumer Fraud Act. [457] The case was dismissed without prejudice on September 27, 2017. [458]

Sling Media Inc. fared better in the Second Circuit, which in November 2017 affirmed the dismissal of a class action complaint against Sling Media that alleged deceptive business practices in connection with Sling's introduction of unwanted advertisements into its television streaming service. [459] In a summary order, the panel affirmed the district court's holding that the complaint and proposed amendments to the complaint failed to plausibly allege a violation of New York General Business Law Section 349, because plaintiffs failed to point to any affirmative statement or omission made by Sling Media that would have misled a reasonable consumer into believing that the service would never include advertisements. [460]

4. Smart Toys

On August 8, 2017, a proposed class action was brought against Viacom by parents of children who, while playing online games via smart phone apps, allegedly had their personal information collected and sold to advertisers. [461] Plaintiffs allege that Viacom makes and markets to children games that collect user data which is then cross-referenced with the child's activity across other apps and platforms and used for targeted advertising. [462] Plaintiffs assert violations of the federal Children's Online Privacy Protection Act and, on behalf of a California subclass, violations of the California constitutional right to privacy. [463]

5. Regulatory Guidance

On June 21, 2017, the FTC released an updated guidance document for complying with the Children's Online Privacy Protection Act ("COPPA"), which explicitly identifies connected toys and other IoT devices as being covered under COPPA. [464] The FTC then issued a clarification on October 23, 2017 that it would not take enforcement action against an operator who—without first obtaining verifiable parental consent—collected an audio file containing a child's voice solely as a replacement for written words, such as to perform a search or fulfill a verbal instruction or request (provided the audio that was sought did not contain personal information), and only maintained the file for the brief time necessary for that purpose. [465] The privacy and data security risks for emerging and novel connected devices were further emphasized when, in July 2017, the FBI warned consumers that internet-connected toys present privacy and safety risks for children. [466]

The FTC has identified IoT as a privacy enforcement priority and has taken several actions against IoT manufacturers. [467] In addition to the private actions against Vizio described above, the FTC also brought an enforcement action against Vizio, asserting that the company had violated the unfairness and deception prongs of Section 5 of the FTC Act and that Vizio's actions caused or were likely to cause "substantial injury" to consumers. [468] In February 2017, Vizio agreed to pay a $2.2 million fine to resolve allegations by the FTC and the New Jersey Attorney General. [469] In addition to the fine, the agreement also required Vizio to obtain affirmative express consent prior to collecting any consumer data. [470]

The rapid adoption of internet-connected devices has spurred action on international as well as state level. The European Union Agency for Network and Information Security has joined several semiconductor makers in calling for baseline privacy and cybersecurity requirements for connected devices. [471] The proposed requirements include certification and labeling of trusted devices. [472] States also continue to explore new legislation to address this issue. One of a number of bills pending in state legislatures is California's SB-327. [473] If passed, it would require disclosure to consumers of the extent to which "connected devices" are capable of collecting biometric data. [474]

I. Civil Litigation: Cybersecurity Insurance

1. State of the Market

Although still a nascent industry, the cybersecurity insurance market is expected to experience massive growth throughout 2018. [475] This anticipated market expansion is based on persistent cyber threats and new state, federal, and international regulatory schemes. [476]

This cybersecurity regulatory fabric includes the already complex web of individual state regulations, as well as a new federal regulatory agency and the European Union's General Data Protection Regulation ("GDPR"). Several states—including New York, [477] California, Illinois, Colorado, and Maryland—already contribute to the vast web of regulatory requirements. [478] For example, as discussed above, a series of class action lawsuits have arisen from Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, presenting new questions for insurers on how cyber liability insurance policies relate to these actions. [479]

The regulation expansion will not only yield industry growth, but will also present significant challenges for insurance companies catering to this complex regulatory landscape. [480] Ultimately, recent figures estimate that "total annual cyber premiums are expected to rise from $2.5 billion in 2017 to $10 billion by 2020." [481]

2. State of the Law – Key Cases

a. Computer Fraud Insurance Provisions

One frequently recurring debate in this year's cases was whether computer fraud insurance provisions covered variations in hacking, intrusions, or cyber-fraud schemes. The Ninth, Sixth, and Second Circuits all heard arguments or decided cases on these issues.

Although each decision depended heavily on the precise wording of an individual insurance policy, several courts held that computer fraud coverage did not apply to email spoofing schemes where the policy holder voluntarily wired money. For example, in *Taylor Lieberman v. Federal Insurance Co.*, the Ninth Circuit held that a policy's coverage for computer fraud did not apply when wire transfers were made in response to a hacker who was masquerading as a client. [482] The court rejected the plaintiff's claims that the fraudulent email constituted an unauthorized entry or trespass into the plaintiff's computer system. [483] The Sixth Circuit recently heard arguments on the scope of a computer fraud policy as well in *American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America* . [484] The litigation was triggered after plaintiff, a tool manufacturer, received an email from a cyber-attacker posing as a vendor and requesting payment. [485] The plaintiff wired the cyber fraudsters $800,000 as a result of the sham. [486] When the insurance company denied coverage, the tooling manufacturer sued. The district court granted summary judgment for the insurance company, 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.'" [487] Relying on the Ninth Circuit's reasoning, the district court adopted the interpretation that the phrase "fraudulently cause a transfer" required the "unauthorized transfer of funds." [488] The

district court therefore concluded that plaintiff did not "suffer a 'direct loss' that was 'directly caused by computer fraud.'" [489] On appeal, petitioner contended that such intervening steps should not be dispositive of the analysis when use of a computer is at the heart of the fraud. [490]

The Second Circuit heard arguments in November 2017 in a very similar case, *Medidata Solutions, Inc. v. Federal Insurance Co*. [491] Cybercriminals spoofed the email account of the company's president, resulting in the wiring of $4.7 million from the plaintiff to the cybercriminals. [492] The insurance company, as in the Sixth Circuit case, disputed whether the insurance agreement's computer fraud provision covered the incident. [493] Here, however, the district court determined that the policy provided coverage for the losses. [494] The court considered that "the fraud on Medidata was achieved by entry into Medidata's email system with spoofed emails armed with a computer code that masked the thief's true identity." [495] And the losses were a direct cause of a computer violation. [496] The *Medidata* court distinguished the Ninth Circuit's decision in *Taylor & Lieberman*, reasoning that, in *Medidata*, "Medidata did not suffer a loss from spoofed emails sent from one of its clients," but rather "[a] thief spoofed emails armed with a computer code into the email system that Medidata used," and that "the fraud caused transfers out of Medidata's own bank account." [497] The district court therefore held that the policy *did in fact* cover the fraud, reasoning that the fraudster's approach in Medidata's case is the type of unauthorized, "deceitful and dishonest access" contemplated by the ruling in *Universal American Corp. v. National Union Fire Insurance Co.* [498] In its amicus brief on appeal, the Surety & Fidelity Association of America contended that "'[o]utwitting of the computer system is a very different risk than misleading the insured's human employees — who have the ability to take reasonable steps to confirm the legitimacy of a wire transfer request or direction received by email — and who then make an authorized transfer based upon such request or direction.'" [499]

In a separate type of scheme, a debit card processor's system flaw allowed pre-paid debit card holders to reuse card balances multiple times. [500] The district court considered whether this scheme constituted a "computer fraud" within the meaning of the policy and under Georgia law. [501] The court held that, because the "cardholders 'used' telephones to provide responses to prompts from a computer that [plaintiff] owned and operated," a computer did not perpetrate the scheme. [502] The computer fraud provision therefore did not cover any losses from the scheme. [503]

b. Litigation Costs

Another significant area of contention was the coverage for data breach litigation costs. For example, the Fifth Circuit recently heard arguments in *Spec's Family Partners, Ltd. v. The Hanover Insurance Co.* where the plaintiff's card payment system experienced two data breaches, prompting litigation between the plaintiff and its third-party transaction service provider. [504] The plaintiff submitted claims to the defendant, its insurance company, to pay for litigation expenses. [505] Defendant refused to pay. [506] In the ensuing case, the district court considered the meaning of the "duty to defend," where plaintiff received demand letters and also instituted its own litigation vis-à-vis the third-party provider. [507] The court looked to the eight corners rule in ascertaining whether the insurer had a duty to defend. [508] That is, the court compared the words of the insurance policy with the allegations of plaintiff's complaint "to determine whether *any* claim asserted in the pleading is potentially within the policy's coverage." [509] Here, the policy provided that the insurer had "the right and duty to defend 'Claim,'

even if the allegations in such 'Claims' are groundless[.]" [510] The definition of a "Claim" included a written demand for damages or non-monetary relief, or "[a]ny complaint or similar pleading initiating a judicial, civil, administrative, regulatory, alternative dispute, or arbitration proceeding[.]" [511] Because the demand letters were not separate claims against plaintiff Spec's specifically, they did not meet the definition of a "claim" under the policy. [512] Moreover, the court agreed with defendant insurer that "the only claim Spec's asserted is [the third-party's] demand for indemnification based on the Merchant Agreement – which is expressly excluded from policy coverage." [513] The court therefore granted the defendant's motion for judgment on the pleadings on all grounds. [514]

In a similar matter, a hospital inadvertently sent out the private information of 20,000 patients to job applicants, triggering a lawsuit. [515] The hospital's insurer then declined to provide a defense in the underlying action because it considered its policy only excess coverage. [516] Upon removal to federal court, the hospital contended that the denial of coverage to cover its defense in the ensuing litigation constituted a breach of contract and a breach of the covenant of good faith. [517] Finally, in *Innovak International, Inc. v. The Hanover Insurance Co.*, the district court held that an insurance company was not responsible for the defense of a database software company where the claims in the underlying action—failure to implement proper security measures—were not the type of claims covered by the insurance policy, which only covered claims for "personal and advertising injury." [518]

J. Fair Credit Reporting Act

Credit agencies and employers continued to face Fair Credit Reporting Act class action claims in 2017, which were on the rise from last year [519] despite continued uncertainty resulting from inconsistent lower-court applications of the Supreme Court's decision in *Spokeo, Inc. v. Robins*. [520] Enacted in 1970, the Fair Credit Reporting Act ("FCRA") promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies and protects consumers from the willful and/or negligent inclusion of inaccurate information in their background check reports. [521] The FCRA provides for penalties of up to $1000 per "willful" violation, actual damages for negligent violations, punitive damages, and attorney's fees. [522]

A substantial verdict against TransUnion awarded this year may spur further litigation regarding the accuracy of credit agency reporting. [523] In June 2017, a California jury awarded $60 million in statutory and punitive damages to a class of more than 8,000 members claiming TransUnion hindered their ability to obtain credit and adversely affected other eligibility decisions by unreasonably linking them with similarly named terrorists and criminals from a government watch list and failing to properly notify them of their rights once discovered. [524] TransUnion has since filed a notice of appeal to the Ninth Circuit. [525]

Meanwhile, courts remain split on how to interpret the FCRA's requirement of "maximum possible accuracy" in credit reports. [526] In an August 2017 ruling, the Eleventh Circuit, in dicta, agreed with the Fourth, Fifth, and D.C. Circuit Courts that the standard requires "information that is both technically accurate and not misleading or incomplete," whereas some courts, including District Courts in Maryland, Connecticut and the Northern District of Alabama, have ruled that the standard requires only that credit reporting agencies report information that is "technically accurate." [527] The Eleventh Circuit

explained that the difference between the two standards is like "the difference between report[ing] that a person was 'involved' in a credit card scam and report[ing] that he was in fact one of the victims of the scam." [528]

Also increasing in frequency are class action suits alleging that employers ran background checks on prospective hires without prior expressed, written consent in "a document that consists solely of the disclosure," as required by the FCRA. [529] With mixed success so far, plaintiffs have pursued litigation against, among others, Amazon, [530] Wells Fargo, [531] Michaels Stores, [532] and Home Depot [533] this year. Many of these cases involve online employment applications that include pages containing FCRA disclosures, putting at issue how to interpret the statute's definition of "a document that consists solely of the disclosure" in a world where more companies are turning to web-based forms. However, while some cases are proceeding, other courts, in light of *Spokeo*, have been dismissing similar suits for the lack of an injury sufficient to confer Article III standing.

III. Government Data Collection

Unsurprisingly, this past year has witnessed continued friction between tech companies and privacy advocates, on the one hand, and law-enforcement and national security entities on the other. Two major decisions are expected from the Supreme Court in the coming months, both addressing the scope of the government's powers under the Stored Communications Act. These cases are described in greater detail below. One major debate in 2017, over the future of the Foreign Intelligence Surveillance Act (FISA), ended with a whimper. Although FISA was set to expire at the end of last year, it is now clear that the status quo will remain in place, if only because lawmakers could not agree about how to amend the law.

A. Challenge to Government "Gag Orders"

As we reported in our 2017 Data Privacy Outlook and Review, Microsoft Corporation sued the U.S. Department of Justice in April 2016 alleging the unconstitutionality of 18 U.S.C. §§ 2703 and 2705(b)—which permit the federal government to issue "[p]reclusion of notice" or "gag" orders preventing cloud storage companies from disclosing government warrants for seizure of user data. [534] These orders, which may last "for such period as the court deems appropriate," *must* be issued upon application by a government agency if a court finds "reason to believe" that disclosure of the warrant at issue will endanger public safety, jeopardize an ongoing investigation, or unduly delay trial. [535] Microsoft stated that it had received over 3,250 such orders in the 20 months ending in May 2016. [536]

A number of organizations filed amicus briefs in support of Microsoft, including a group of law professors represented in part by Gibson Dunn; [537] civil liberties organizations such as the Electronic Frontier Foundation; [538] news organizations, including the Associated Press and Fox News; [539] and technology companies, including Apple and Mozilla. [540]

In February 2017, the District Court for the Western District of Washington partially denied the government's motion to dismiss Microsoft's claims, finding that the gag orders' indefinite limitation on Microsoft's ability to speak about warrants issued under § 2703 was a First Amendment injury sufficient to support standing. [541] The court also found that Microsoft had sufficiently stated a claim that indefinite § 2705(b) gag orders were unconstitutional prior restraints and content-based restrictions on

speech, whether subject to a strict scrutiny analysis or a lesser standard of review. [542] However, the court rejected Microsoft's effort to assert its customers' Fourth Amendment right against unreasonable search and seizure, finding third-party standing disfavored by the Supreme Court and the Ninth Circuit in a wide range of contexts, despite acknowledging that "some of Microsoft's customers will be practically unable to vindicate their own Fourth Amendment rights." [543]

Following the lawsuit, the Office of the Deputy Attorney General issued new guidance to federal prosecutors last October that substantially tightens requirements for obtaining protective orders under § 2705(b). [544] Most notably, the new policy bars Department of Justice attorneys from seeking protective orders that delay notice for more than one year "[b]arring exceptional circumstances." [545] It also requires that prosecutors explain which of the five conditions set forth in subsection (b) apply to the case at hand and seek protective orders under § 2705(b) only "when circumstances require." In response to the policy, Microsoft promptly filed an unopposed motion to voluntarily dismiss its lawsuit, in which it acknowledged that "the new Policy significantly improves DOJ practices under Section 2705(b)," and the motion was granted. [546]

B. *Carpenter v. United States* and the Collection of Cell Phone Data

On November 29, 2017, the Supreme Court heard oral argument in *Carpenter v. United States*, a case addressing another aspect of the Stored Communications Act. Specifically, the Court is considering whether the government violates the Fourth Amendment by obtaining historical cell tower location data pursuant to a court order issued under 18 U.S.C. § 2703(d) rather than a probable cause warrant. *Carpenter* is expected to test the limits of the so-called "third-party doctrine," which holds that government acquisition of information voluntarily provided to a third party—such as call records—is not a search for Fourth Amendment purposes and thus does not require a warrant.

The *Carpenter* petitioner was convicted of robbing several stores in 2010 and 2011. [547] During its investigation, the government obtained court orders pursuant to § 2703(d) to obtain "cell site information for [petitioner's] telephone," which identified the cell towers to which petitioner's phone connected when making and receiving calls during a 127-day period encompassing the robberies. [548] This data permitted only a rough estimation of petitioner's location at the times of the calls, but nonetheless allowed the government to place petitioner's phone in the vicinities of the robberies when they occurred. [549] Petitioner moved to suppress the cell-site records, arguing that their acquisition without a probable cause warrant violated the Fourth Amendment, and the district court denied his motion. [550] On appeal, the Sixth Circuit affirmed, analogizing cell tower information to "mailing addresses, phone numbers, and IP addresses"—non-content information used to "facilitate personal communications" in which a person has no reasonable expectation of privacy. [551] In reaching its decision, the Sixth Circuit relied on two landmark third-party doctrine precedents: *Smith v. Maryland*, which held that use of a "pen register" to capture dialed telephone numbers did not implicate a reasonable expectation of privacy, [552] and *United States v. Miller*, which held that a customer had no reasonable expectation of privacy in account statements, deposit slips, and cancelled checks held by a bank. [553]

On appeal to the Supreme Court, the government also cites *Smith* and *Miller* in arguing that the third-party doctrine encompasses cell site data, and that its acquisition was not a Fourth Amendment search

of petitioner. [554] In the alternative, the government argues that if that acquisition *did* constitute a search, it was reasonable in light of the 18 U.S.C. § 2703(d) requirement that the government show "specific articulable facts" to support a court order and the importance of cell site records to law enforcement investigations. [555] Petitioner argues that the retrospective acquisition of long-term cell site data *is* a Fourth Amendment search, analogizing it to "longer term GPS monitoring." [556] Petitioner also urges the Court to look to the future, asserting that "the rule [the Court] adopt[s] must take account of more sophisticated systems that are already in use or development," and noting that cell site data is becoming both more precise and more voluminous. [557]

The case has garnered significant public attention, with a variety of amici filing briefs in support of petitioner (including, among others, the Center for Democracy and Technology, [558] the Competitive Enterprise Institute, [559] the Electronic Privacy Information Center, [560] the Reporters Committee for Freedom of the Press and a group of nineteen media organizations, [561] a group of 42 privacy and criminal procedure scholars, [562] and a group of 19 technology experts [563]), the government (including, among others, the National District Attorneys Association, [564] a group of 19 state Attorneys General, [565] and Professor Orin Kerr [566]), and of neither party (a group of 15 technology companies including Apple, Google, Facebook, Microsoft, Twitter, Verizon, and others [567]).

C. Electronic Communications Privacy Act Reform Efforts

There are currently two bills pending before Congress to reform the ECPA in ways that would address the issues raised by both the Microsoft gag order litigation and the warrantless collection of geolocation data in *Carpenter v. United States*. The Email Privacy Act, [568] introduced by Senators Patrick Leahy (D-Vermont), Mike Lee (R-Utah), and others on July 27, 2017, is a companion bill to the Email Privacy Act passed by the House of Representatives by voice vote in February. [569] Most significantly, the Email Privacy Act would require law enforcement to obtain a probable cause warrant to acquire the content of *all* emails or other electronic communications (under 18 U.S.C. § 2703 the government can currently obtain the contents of electronic communications that are more than 180 days old via a court order). [570]

Also on July 27, Senators Leahy and Lee introduced the ECPA Modernization Act of 2017. [571] Like the Email Privacy Act, this bill would require a warrant for acquisition of electronic communication content, [572] but would also add a variety of additional reforms. First, it would substantially amend 18 U.S.C. § 2705(b) by adding a requirement that a court issuing a § 2705(b) nondisclosure order find "specific articulable facts" supporting its issuance, and by limiting § 2705(b) nondisclosure orders to 90 days (extendable by one or more periods of not more than 90 days). [573] This change would eliminate the government's ability to obtain nondisclosure orders of indefinite duration—one of the central issues identified by Microsoft in challenging § 2705(d) and addressed in the Deputy Attorney General's subsequent guidance document that generally bars "gag" orders lasting more than one year. [574]

Second, the ECPA Modernization Act would amend 18 U.S.C. § 2703 to permit government officials to obtain "stored geolocation information" [575] only pursuant to a warrant supported by probable cause, and would require notice to the subscriber whose geolocation information was accessed within ten days. [576] Under current law, acquisition of stored geolocation information does not require a warrant, but

rather only a court order supported by "specific articulable facts" showing that the information is "relevant and material to an ongoing criminal investigation." [577] The constitutionality of warrantless acquisition of this kind of information is the question currently before the Supreme Court in *Carpenter v. United States.*

Other significant changes proposed in the ECPA Modernization Act include requiring the government to notify a subscriber within 10 days of obtaining the contents of the subscriber's wire or electronic communications or geolocation information from a third-party cloud storage provider, [578] and explicitly providing a suppression remedy for cloud content or stored or real-time geolocation information obtained without a warrant or otherwise in violation of the law. [579]

A variety of research, advocacy, and technology industry groups and companies have publicly expressed support for the ECPA Modernization Act of 2017, including the Electronic Frontier Foundation, [580] the American Civil Liberties Union, [581] FreedomWorks, [582] Citizens Against Government Waste, [583] the Consumer Technology Association, [584] the Center for Democracy and Technology, [585] the National Association of Criminal Defense Lawyers, [586] and Microsoft. [587]

D. Device Unlocking

The use of biometric security systems—such as facial recognition, fingerprint unlocking, and iris scanning—in mobile devices has become increasingly prevalent in recent years, and has received even greater attention with the introduction of Apple's Face ID technology in September 2017. While there remains some division among courts about whether police violate the Fifth Amendment by compelling a suspect to unlock an electronic device using a traditional passcode, [588] courts have recently held—although not without exception—that unlocking a device using a thumbprint is not "testimonial" and thus does not implicate a suspect's Fifth Amendment right against self-incrimination. [589] There is currently no case law addressing whether the government may compel a suspect to unlock a device using facial features as opposed to a thumbprint, but the same reasoning is likely to apply. Thus, while biometric security may offer sufficient protection from intrusion by hackers, it may offer less protection against government access than traditional security measures such as passcodes or PINs. A new feature in Apple's most recent operating system iOS 11 would provide one means of addressing this concern. Pressing the power button on an iOS 11-equipped device five times in rapid succession disables biometric unlocking and thus requires a PIN or passcode to unlock it. [590]

E. Extraterritoriality of Subpoenas and Warrants

Before the end of the 2017-18 term, the Supreme Court will determine the scope of the government's power to obtain information stored overseas under the Stored Communications Act ("SCA"). This case, now styled *United States v. Microsoft, Inc.*, arose in December 2013, when the Southern District of New York issued a warrant under Section 2703 of the SCA requiring Microsoft to produce the contents of an email account. [591] Microsoft filed a motion to quash, arguing that the data was stored in a server in Ireland and the warrant was an inappropriate extraterritorial application of the SCA. [592] On April 25, 2014, the district court denied Microsoft's motion to quash, holding that a warrant under Section 2703 requires the recipient to produce all information in its possession, custody, or control, even if the

information is stored abroad. [593] On July 14, 2016, the Second Circuit reversed and remanded on appeal. [594] The court concluded that SCA warrants are not equivalent to subpoenas which may require the production of communications stored overseas, and further held that the case involved an extraterritorial application of the statute because the focus of the SCA is on privacy and a privacy invasion occurs where a customer's content is accessed. [595]

The government requested rehearing en banc. On January 24, 2017, the Second Circuit denied the motion in a split four-to-four decision. [596] The concurring opinion reiterated the view that the SCA's focus is on privacy and that the statute protects privacy at the place that data is stored. [597] Four judges, however, authored dissents, each taking issue with a distinct aspect of Microsoft's argument. [598] In particular, Judge Jacobs rejected Microsoft's analogy to paper documents and reasoned that it is irrelevant where the contents are stored if they are accessible in the US; [599] Judge Cabranes found the conduct at issue to be disclosure, not access, and cautioned that the panel's decision burdened legitimate law enforcement efforts [600] ; and Judge Droney opined that there are no extraterritoriality concerns because the service provider is located domestically. [601]

Since the Second Circuit's decision, district courts in other circuits have taken the opposing approach. The District of the District of Columbia, the Northern District of California, and the Eastern District of Pennsylvania each ordered Google to comply with SCA warrants that were directed to the contents of email accounts stored overseas. [602] The courts found that the focus of the SCA is disclosure and that whether a service provider must produce records if it has sufficient control over the evidence, regardless of where the records are located. [603]

On October 16, 2017, the Supreme Court granted certiorari. [604] In its brief filed on December 6, 2017, the government first argues that the focus of Section 2703 is on the disclosure of information, not storage. [605] Even if privacy is the focus of the provision, no search or seizure would occur in Ireland because Microsoft does not interfere with a customer's possessory interests or reasonable expectation of privacy when it gathers or moves materials in its control. [606] Rather, any invasion to privacy would occur domestically, when Microsoft discloses information to a third party. [607] Next, the government asserts that an SCA warrant resembles a subpoena because it is directed at a person rather than a place, and Microsoft thus must produce all documents under its control. [608] Lastly, the government contends that its ability to collect information for legitimate law enforcement purposes should not be subject to a company's business decision of where to store its data. [609]

On January 11, 2018, Microsoft filed its brief, in which it argues that the SCA's focus is where electronic communications are stored and that a search and seizure occurs in the jurisdiction of the storage. [610] Thus, according to Miscrosoft, the disclosure of communications stored abroad is an impermissible extraterritorial application of the SCA. [611] Oral argument is scheduled for February 27, 2018, and a decision will likely follow this summer.

F. Collection of Records from Third-Party Cloud Providers

On December 13, 2017, the Computer Crime and Intellectual Property Section of the Department of Justice issued internal guidance that instructs prosecutors to request electronic records directly from

companies and not third-party cloud service providers. [612] Compelling information from cloud computing services may raise several complications, such as delays and the inability of the cloud provider to preserve, access, extract, and decrypt the data. [613] The guidance permits exceptions if law enforcement believes the company is unwilling to comply, is engaged in criminal conduct, or is unable to disclose the necessary information. [614] In response to the memorandum, Microsoft praised the policy as "a win" for cloud and enterprise customers. [615]

G. Foreign Intelligence Surveillance Act Section 702

The Foreign Intelligence Surveillance Act (FISA) [616] was passed in 1978 and amended in 2008. FISA was enacted in order to allow the United States government to conduct electronic surveillance "to acquire foreign intelligence information." [617] Foreign intelligence information is defined in the act as information that relates to terrorism, an attack by a foreign power, or national defense generally. [618] The Act established a tribunal – the Foreign Intelligence Surveillance Court [619] – to decide based on classified ex parte proceedings whether to approve government requests to collect data through FISA. The FISA Court famously approved the National Security Agency's PRISM Program, which allowed the agency to clandestinely collect certain data on American citizens from American internet companies, such as Google. [620]

FISA Section 702 specifically allows the U.S. government to target the electronic communications of persons reasonably believed to be outside the United States for intelligence collection without a warrant. The data collected often includes the communications of American citizens who interact with targeted foreigners, so-called "incidental collection." [621] Some believe FISA, including Section 702, is constitutionally sufficient in light of the need to protect U.S. national security, [622] while others believe that the Act violates the First and Fourth Amendments to the Constitution. [623] This controversial law was set to expire in January 2018 unless reauthorized by Congress. Both the Senate and House reauthorized Section 702 for an additional six years without any changes, and President Trump signed the bill into law on January 19. [624]

The past year had seen numerous attempts in the House and Senate to reauthorize or overhaul FISA Section 702. Last October, the Senate Intelligence Committee voted in favor of sending the FISA Amendments Reauthorization Act of 2017 – which was said by its drafters to contain greater protections to civil liberties while maintaining FISA as a powerful tool for national security – to the full Senate. [625] The proposed bill would have required law enforcement to obtain court approval before using information gathered about U.S. citizens in the course of conducting surveillance on foreign nationals, among other changes. [626] Another FISA reauthorization bill, which passed through the House Intelligence Committee in December 2017 and similarly contained additional restrictions on the use of data collected about U.S. citizens, would have renewed Section 702 for four more years, to the end of 2021. [627] However, the January 2018 reauthorization of FISA closed the book on the attempts to amend the law to include greater constitutional protections.

Congress' eleventh-hour reauthorization of FISA after months of debate generated uncertainty around the role of the Act in national defense. The debate over the constitutionality of FISA is sure to continue and may even impact the 2020 presidential election.

IV. International Regulation of Privacy and Data security

We address international developments in more detail in our separate International Cybersecurity and Data Privacy Outlook and Review, but below we highlight several international developments that are likely to have important implications for U.S companies.

A. The European Union

1. General Data Protection Regulation ("GDPR")

One of the most important and pressing issues for U.S.-based companies over the coming year is the upcoming implementation and enforcement of the GDPR. [628] For a more complete overview, please see our recently published primer specifically on the GDPR, accessible here . But as an introduction, here is a quick run-down of some of the most salient facets of the GDPR that are relevant to U.S.-based companies.

- The GDPR requires compliance by all companies that process personal data of data subjects within the EU, regardless of whether the company is located in the EU. [629] It also requires compliance by companies that process data related to monitoring behavior within the EU. [630] Most international companies will therefore be subject to the GDPR.

- The GDPR establishes a high bar for ensuring that a data subject has consented voluntarily to a company's processing of the subject's personal data. A request for consent cannot be obtained through pressure and must be "clearly distinguishable" from other matters in a written agreement. [631] The data subject has the right to withdraw consent at any time and must be informed of this right when initially granting consent. [632] These standards are more stringent than the U.S. standards.

- If a company subject to the GDPR performs data processing that will likely entail a high risk to individual privacy rights, the company must conduct a data protection impact assessment ("DPIA"). [633] The GDPR recommends a DPIA, in particular, when a company is using new technologies. [634] The DPIA must include a detailed description of the processing operations, an assessment of the necessity and proportionality of the operations relative to their purpose, an assessment of the rights of the subjects, and the measures that will be implemented to protect those rights. [635]

- The GDPR ensures that its protections will not be undermined by the transfer of data outside the EU or to international organizations that lack the protections of the GDPR. Data transfers can only take place under the GDPR's guidelines. [636] Data transfers to the U.S. from the EU are currently permissible under the EU-U.S. Privacy Shield, discussed below, as well as under Binding Corporate Rules ("BCRs") and the use of model contractual clauses.

- It remains unclear exactly how substantial penalties under the GDPR will be after enforcement begins on May 25, 2018. Individual countries will be responsible for enforcing the GDPR within their borders, so enforcement likely will vary. Notably, the GDPR authorizes substantial

penalties for non-compliance—up to 4% of a company's annual global turnover or €20 million, whichever is greater. [637]

2. EU-U.S. Privacy Shield

As noted above, one way that a company may comply with the EU's requirements for secure data transfers is through the EU-U.S. Privacy Shield Framework. Administered in the U.S. by the Department of Commerce, the Privacy Shield allows companies to participate voluntarily by establishing a commitment to privacy compliance and self-certifying annually.

The EU-U.S. Privacy Shield has been challenged by groups in Europe that claim its protections are inadequate. But on October 18, 2017, the EU Commission published a report that established that the Privacy Shield, unlike the Safe Harbor framework that preceded it, "ensures an adequate level of protection for personal data that has been transferred from the European Union to organi[z]ations in the U.S." [638] Thus, as of this publication, the Privacy Shield stands as a valid option for companies to comply with the GDPR.

However, the Commission also noted that "the practical implementation of the Privacy Shield framework can be further improved in order to ensure that the guarantees and safeguards provided therein continue to function as intended." [639] The Commission will continue to review the adequacy of the Privacy Shield annually and has provided some recommendations for the U.S. in maintaining the Privacy Shield's adequacy. [640] For now, participation in the Privacy Shield can protect companies that perform data transfers between the EU and the U.S. But companies must be sure they actually are adhering to the Privacy Shield, and not merely paying lip service to it. Indeed, U.S. regulators at the FTC have already taken action against several companies that allegedly deceived consumers by falsely claiming participation in the Privacy Shield framework. [641]

B. China and Other International Developments

In an increasingly connected world, 2017 also saw many countries outside of the United States try to get ahead of the challenges within the cybersecurity and data protection landscape. Several international developments bear brief mention here:

- On June 1, 2017, China's Cybersecurity Law went into effect, becoming the first comprehensive Chinese law to regulate how companies manage and protect digital information. The law also imposes significant restrictions on the transfer of certain data outside of the mainland (data localization) enabling government access to such data before it is exported. [642]

  Despite protests and petitions by governments and multinational companies, the implementation of the Cybersecurity Law continues to progress with the aim of regulating the behavior of many companies in protecting digital information. [643] While the stated objective is to protect personal information and individual privacy, and according to a government statement in China Daily, a state media outlet, to "effectively safeguard national cyberspace sovereignty and security," the law in effect gives the Chinese government unprecedented access to network data for essentially all companies in the business of information technology. [644] Notably, key

components of the law disproportionately affect multinationals because the data localization requirement obligates international companies to store data domestically and undergo a security assessment by supervisory authorities for important data that needs to be exported out of China. Though the law imposes more stringent rules on critical information infrastructure operators (whose information could compromise national security or public welfare) in contrast to network operators (whose information capabilities could include virtually all businesses using modern technology), the law effectively subjects a majority of companies to government oversight. As a consequence, the reality for many foreign companies is that these requirements would likely be onerous, will increase the costs of doing business in China, and will heighten the risk of exposure to industrial espionage. [645] Despite the release of additional draft guidelines meant to clarify certain provisions of the law, there is a general outlook that the law is still a work in progress, with the scope and definition still vague and uncertain. [646] Nonetheless, companies should endeavor to assess their data and information management operations to evaluate the risks of the expanding scope of the data protection law as well as their risk appetite for compliance with the Chinese government's access to their network data.

- With the growing threat of hacking and identity theft, the Personal Data Protection Commission of Singapore issued proposed advisory guidelines on November 7, 2017 for the collection and use of national registration identification numbers. The guidance, which covers a great deal of personal and biometric data, emphasized the obligations of companies to ensure policies and practices are in place to meet the obligations for data protection under the Personal Data Protection Act of 2012. The Commission is giving businesses and organizations twelve months from publication to review their processes and implement necessary changes to ensure compliance. [647]

- Several other countries, such as Australia and Turkey, also sought to address privacy issues and published important guidelines regarding procedures for deleting, destroying, and anonymizing personal data. Other countries like Argentina forged ahead with an overhaul of the country's data protection regime by publishing a draft data protection bill that would align the country's privacy laws with the GDPR requirements of the European Union. [648]

- There has also been civic engagement with the public as a number of countries solicited public comments to certain proposed regulations. For example, Canada opened up for comments a proposed regulation that would mandate reporting of privacy breaches under its Personal Information Protection and Electronic Documents Act of 2015, while India recently issued a white paper inviting comments that would inform the legal framework for drafting a data protection bill to "ensure growth of the digital economy while keeping personal data of citizens secure and protected." [649]

V. Conclusion

We expect 2018 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.

---

[1] Susan Heavey and Dustin Volz, *FTC Probes Equifax, Top Democrat Likens It To Enron*, Reuters (Sept. 14, 2017), *available at* https://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX.

[2] Press Release, Federal Trade Commission, *Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That it Violated Financial Privacy and Security Rules* (Aug. 29, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges.

[3] Final Order at 1, *In the Matter of LabMD, Inc.*, No. 9357 (F.T.C. July 28, 2016).

[4] Press Release, Federal Trade Commission, *FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy* (Aug. 29, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

[5] Initial Decision at 13–14, *In the Matter of LabMD, Inc.*, No. 9357 (F.T.C. Nov. 13, 2015).

[6] *LabMD, Inc. v. Fed. Trade Comm'n* , 678 F. App'x 816, 817 (11th Cir. 2016).

[7] Press Release, Federal Trade Commission, *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras* (Jan. 5, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.

[8] *Fed. Trade Comm'n v. D-Link Sys., Inc.* , No. 3:17-CV-00039-JD, 2017 WL 4150873, at *1 (N.D. Cal. Sept. 19, 2017).

[9] *Id* . at *5.

[10] *Id* .

[11] Press Release, Federal Trade Commission, *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* (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.

[12] Press Release, Federal Trade Commission, *Lenovo Settles FTC Charges it Harmed Consumers with Preinstalled Software on its Laptops that Compromised Online Security* (Sept. 5, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

[13] Press Release, Federal Trade Commission, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases* (Sept. 19, 2017), *available at* https://www.ftc.gov/public-statements/2017/09/painting-privacy-landscape-informational-injury-ftc-privacy-data-security.

[14] *Id.*

[15] Bryan Koenig, *FTC's Definition Of Cyber Injury Getting Broader, Chief Says* , Law360 (May 17, 2017), *available at* https://www.law360.com/articles/925071/ftc-s-definition-of-cyber-injury-getting-broader-chief-says.

[16] Allison Grande, *Biz Groups Push FTC To Avoid 'Theoretical' Privacy Harms*, Law360 (Nov. 1, 2017), *available at* https://www.law360.com/articles/980724/biz-groups-push-ftc-to-avoid-theoretical-privacy-harms .

[17] *Fed. Trade Comm'n v. AT&T Mobility LLC* , 864 F.3d 995 (9th Cir. 2017).

[18] Press Release, Department of Health and Human Services,*OCR Launches Phase 2 of HIPAA Audit Program*, (no date), *available at* http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/ .

[19] Press Release, Department of Health and Human Services, *$5.5 million HIPAA settlement shines light on the importance of audit controls* (Feb. 16, 2017), *available at* https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html .

[20] Press Release, Department of Health and Human Services, *Lack of timely action risks security and costs money* (Feb. 1, 2017), *available at* https://www.hhs.gov/about/news/2017/02/01/lack-timely-action-risks-security-and-costs-money.html .

[21] Press Release, Department of Health and Human Services, *Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k* (May 23, 2017), *available at* https://www.hhs.gov/about/news/2017/05/23/careless-handling-hiv-information-costs-entity.html .

[22] Press Release, Department of Health and Human Services, *First HIPAA enforcement action for lack of timely breach notification settles for $475,000* (Jan. 9, 2017), *available at* http://wayback.archive-it.org/3926/20170127111957/https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html

[23] Press Release, Department of Health and Human Services, *$2.5 million settlement shows that not understanding HIPAA requirements creates risk* (Apr. 24, 2017), *available at* https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html .

[24] Press Release, Department of Health and Human Services, *Failure to protect the health records of millions of persons costs entity millions of dollars* (Dec. 28, 2017), *available at* https://www.hhs.gov/about/news/2017/12/28/failure-to-protect-the-health-records-of-millions-of-persons-costs-entity-millions-of-dollars.html .

[25] Department of Health and Human Services, *How HIPAA Allows Doctors to Respond to the Opioid Crisis* (no date), *available at* https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf .

[26] SEC Division of Corporation Finance, CF Disclosure Guidance:*Topic No. 2—Cybersecurity* (Oct. 13, 2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm .

[27] Ed Beeson, *SEC Likely To Revisit Cybersecurity Guidance, Official Says* , Law360 (Nov. 9, 2017, 8:48 PM), https://www.law360.com/cybersecurity-privacy/articles/983742/sec-likely-to-revisit-cybersecurity-guidance-official-says .

[28] Jimmy Hoover, *SEC Suits Over Cyber Reporting Could Be On Horizon*, Law360 (Apr. 20, 2017, 1:25 PM), https://www.law360.com/privacy/articles/915377/sec-suits-over-cyber-reporting-could-be-on-horizon .

[29] Beeson, *supra* note 27.

[30] *Id.*

[31] Chris Isidore, *Equifax is investigating executive stock sales*, CNN Money (Sept. 29, 2017, 3:19 PM), http://money.cnn.com/2017/09/29/news/companies/equifax-investigation/index.html .

[32] Tom Schoenberg, Anders Melin, and Matt Robinson, *Equifax Stock Sales Are the Focus of U.S. Criminal Probe*, Bloomberg (Sept. 18, 2017, 12:20 PM), https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe .

[33] Equifax Inc., Quarterly Report (Form 10-Q) at 40 (Nov. 9, 2017), available at https://otp.tools.investis.com/clients/us/equifax/SEC/sec-show.aspx?Type=html&FilingId=12372346&CIK=0000033185&Index=10000 ; *see also* Hayley Tsukayama, *Equifax faces hundreds of class-action lawsuits and an SEC subpoena over the way it handled its data breach* , Washington Post (Nov. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach/?utm_term=.ceebfb8dc054 .

[34] Public Statement, SEC Chairman Jay Clayton,*Statement on Cybersecurity*, SEC (Sept. 20, 2017), *available at* https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20#_ftnref10 .

[35] *Id.*

[36] Press Release, SEC, *SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors* , SEC (Sept. 25, 2017), *available at* https://www.sec.gov/news/press-release/2017-176 .

[37] Press Release, SEC, *SEC Emergency Action Halts ICO Scam*, SEC (Dec. 4, 2017), *available at* https://www.sec.gov/news/press-release/2017-219 .

[38] *Id.*

[39] The SEC alleges that Paradis-Royer, believed to be Lacroix's romantic partner, helped to cover up the scheme when she, amongst other conduct, registered payments in her name, and attempted to resist Quebec authorities when they arrived at Lacroix and Paradis-Royer's residence and warn Lacroix of the search. *See* Compl., ECF No. 1, *SEC v. PlexCorps et. al.*, 1:17-CV-07007, at ¶¶ 24, 63, 92 (E.D.N.Y. Dec 1, 2017), *available at* https://www.sec.gov/litigation/complants/2017/comp-pr2017-219.pdf .

[40] *See* Compl., ECF No. 1, *SEC v. PlexCorps et. al.*, 1:17-CV-07007 (E.D.N.Y. Dec 1, 2017), *available at* https://www.sec.gov/litigation/complants/2017/comp-pr2017-219.pdf ; *see also* Press Release, SEC, *supra* note 37.

[41] Press Release, SEC, *supra* note 37.

[42] David Shepardson, *Trump Signs Repeal of U.S. Broadband Privacy Rules*, Reuters (April 3, 2017, 7:50 PM), *available at* https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR .

[43] *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report & Order ("Commission Order"), FCC Dkt. No. 16-148 (Nov. 2, 2016), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1103/FCC-16-148A1.pdf.

[44] David Shepardson, *FCC Approves TV Technology that Gives Better Pictures but Less Privacy* , Reuters (Nov. 16, 2017, 3:25 PM), *available at* https://www.reuters.com/article/us-usa-television-technology/fcc-approves-tv-technology-that-gives-better-pictures-but-less-privacy-idUSKBN1DG2XF .

[45] *See* John Eggerton, *Dingell has Privacy Concerns over ATSC 3.0*, Broadcasting Cable, (Nov. 8, 2017, 4:52 PM), http://www.broadcastingcable.com/news/washington/dingell-has-privacy-concerns-over-atsc-30/169962 .

[46] SS7 is a signaling protocol that supports call setup, routing, exchange, and billing functions in communications networks by transmitting messages between fixed and mobile service providers. *See FCC's Public Safety & Homeland Security Bureau Encourages Implementation of CSRIC Signaling System 7 Security Best Practices* , DA-17-799 (Aug. 24, 2017), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwi8_tXflYrYAhXC5CYKHTC4BroQFggwMAE&url=https%3A%2F%2Fapps.fcc.gov%2Fedocs_public%2Fattachmatch%2FDA-17-799A1.docx&usg=

AOvVaw3NB4Lc5YhzWjjTAxZv9Hss ; *see also* Jenna Ebersole, *Dem Lawmakers Urge FCC Action On Cellphone Cybersecurity*, Law360 (March 28, 2017, 8:05 PM), https://www.law360.com/articles/906956/dem-lawmakers-urge-fcc-action-on-cellphone-cybersecurity .

[47] FCC, Order, Straight Path Communications Inc., Ultimate Parent Company of Straight Path Spectrum, LLC, Straight Path Spectrum LLC, File No. EC-SED-16-00022575, Acct. No. 201732100003, FRN: 0022779334 (Jan. 12, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DA-17-40A1.pdf.

[48] Stephen Lawson, *FCC looks to higher frequencies for 5G mobile* (Oct. 22, 2015, 1:44 PM), https://www.computerworld.com/article/2996149/mobile-wireless/fcc-looks-to-higher-frequencies-for-5g-mobile.html .

[49] FCC, Order, Straight Path Communications Inc., Ultimate Parent Company of Straight Path Spectrum, LLC, Straight Path Spectrum LLC, File No. EC-SED-16-00022575, Acct. No. 201732100003, FRN: 0022779334 (Jan. 12, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DA-17-40A1.pdf.

[50] Blog of FCC Chairman Ajit Pai, *Consumer Protection Month at the FCC* (June 22, 2017, 2:20 PM), https://www.fcc.gov/news-events/blog/2017/06/22/consumer-protection-month-fcc .

[51] Press Release, Federal Communications Commission, Robocall Scammer Faces $120 Million Proposed Fine for Massive Caller ID Spoofing Operation (June 22, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-345470A1.pdf .

[52] Kelcee Griffis, *FCC Fines Co. $2.8M For Powering Robocalls To Cellphones*, Law360 (July 13, 2017, 4:27 PM), https://www.law360.com/articles/944001/fcc-fines-co-2-8m-for-powering-robocalls-to-cellphones ; Press Release, Federal Communications Commission, FCC Proposes $82 Million Fine for Spoofed Telemarketing Robocalls (Aug. 3, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-346059A1.pdf.

[53] Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Consumer Financial Protection Bureau (Oct. 18, 2017), *available at* http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[54] Stakeholder Insights that Inform the Consumer Protection Principles, Consumer Financial Protection Bureau (October 18, 2017), *available at* http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[55] *See supra* note 54.

[56] Press Release, Bureau Seeks to Ensure a Workable Data Aggregation Market that Gives Consumers Protection and Value (Oct. 18, 2017), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

[57] *Id.*

[58] *See supra* note 54.

[59] Assurance of Voluntary Compliance, *In the Matter of Investigation by Eric T. Schneiderman, Attorney General of the State of New York, of Target Corporation* , No. 17-094 (May 15, 2017) , *available at* https://ag.ny.gov/sites/default/files/nyag_target_settlement.pdf

[60] *Id* .; *see also* Press Release, A.G. Schneiderman Announces $18.5 Million Multi-State Settlement With Target Corporation over 2013 Data Breach (May 23, 2017), *available at* https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over.

[61] Assurance of Voluntary Compliance, *In Re Nationwide Mutual Ins. Co. and Allied Prop. & Casualty Ins. Co* ., (Aug. 3, 2017), *available at* https://ag.ny.gov/sites/default/files/nationwide-aod.pdf; *see also* Press Release, A.G. Schneiderman Announces $5.5 Million Multi-State Settlement With Nationwide Mutual Insurance Company Over 2012 Data Breach (Aug. 9, 2017), *available at* https://ag.ny.gov/press-release/ag-schneiderman-announces-55-million-multi-state-settlement-nationwide-mutual.

[62] *Id* .

[63] Press Release, Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security (Sept. 5, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

[64] Press Release, Attorney General Becerra Announces $3.5M Settlement with Lenovo for Preinstalling Software that Compromised Security of its Computers (Sept. 5, 2017), *available at* https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-35m-settlement-lenovo-preinstalling-software.

[65] Press Release, AG's Office Alleges Company Failed to Protect Personal Information of Nearly Three Million Massachusetts Residents, Despite Knowing its System was Vulnerable to Hackers (Sept. 19, 2017), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-09-19-equifax-lawsuit.html;*see also* Complaint, *Commonwealth of Massachusetts v. Equifax, Inc*., (Suffolk Sup. Ct. Sept. 19, 2017).

[66] Memorandum In Support of Plaintiffs' Motion For Transfer of Actions to the Northern District of Georgia And For Consolidation Pursuant to 28 U.S.C. 1407, *In Re: Equifax Inc., Consumer Data Security Breach Litigation* , MDL Dkt. No. 2800 (Judicial panel on Multi-district Litigation, Sept. 11, 2017), *available at*: http://www.almcms.com/contrib/content/uploads/sites/292/2017/09/Equifax-MDL-motion.pdf.

[67] Press Release, Attorney General Becerra Announces $2 Million Settlement Involving Santa Barbara-based Cottage Health System Over Failure to Protect Patient Medical Records (Nov. 22, 2017), *available at* https://www.oag.ca.gov/news/press-releases/attorney-general-becerra-announces-2-million-settlement-involving-santa-barbara.

[68] *Id .*; *see also* Complaint for Injunction, Civil Penalties, and Other Equitable Relief, *California v. Cottage Health et al .*, No. 17CV05269 (Sup. Ct. County of Santa Barbara, November 15, 2017), *available at* https://www.oag.ca.gov/system/files/attachments/press_releases/Conformed%20Cottage%20Complaint%20SIGNED.PDF.

[69] Stipulation for Entry of Final Judgment and Permanent Injunction, *California v. Cottage Health, et al.*, No. 17CV05269 (Sup. Ct. County of Santa Barbara, November 15, 2017).

[70] *Id .*

[71] Press Release, A.G. Schneiderman Announces $700,000 Joint Settlement With Hilton After Data Breach Exposed Hundreds of Thousands of Credit Card Numbers (Oct. 31, 2017), *available at* https://ag.ny.gov/press-release/ag-schneiderman-announces-700000-joint-settlement-hilton-after-data-breach-exposed .

[72] *Id .*; N. Y. Gen. Bus. Law § 899-aa(2) (McKinney 2017).

[73] Press Release, New Jersey Division of Consumer Affairs, Federal Trade Commission Reach $2.5 Million Settlement with Smart TV Manufacturer to Settle Allegations of Invasive Data Collection (Feb. 6, 2017), *available at* http://nj.gov/oag/newsreleases17/pr20170206a.html.

[74] *Id .*; *see also* Stipulated Order for Permanent Injunction and Monetary Judgment, *Federal Trade Commission, et al. v. Vizio, Inc.*, No. 2:17-cv-00758 (D. N.J. Feb. 6, 2017), *available at* http://nj.gov/oag/newsreleases17/Vizio-Order.pdf.

[75] *Id .*

[76] Washington State Attorney General's Office, 2017 Data Breach Report, *available at* http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Home/Safeguarding_Consumers/Data_Breach/2017%20Data%20Breach%20Report%20Final.pdf.

[77] 23 NYCRR 500, *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[78] *Id .*

[79] *Id . See also Key Dates under New York's Cybersecurity Regulation (23 NYCRR Part 500)* , N.Y. Dep't of Fin. Servs., http://www.dfs.ny.gov/about/cybersecurity.htm (last visited Jan. 23, 2018).

[80] *Id.*

[81] *Proposed Financial Services Regulations* , N.Y. Dep't of Fin. Servs., http://www.dfs.ny.gov/legal/regulations/proposed/propdfs.htm (last visited Jan. 23, 2018).

[82] Executive Order 13,800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* , May 11, 2017.

[83] *Id.* at 1.

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

[85] *Id.* at 4.

[86] See Press Release, Final IT Modernization Report, Dec. 13, 2017, *available at* https://www.whitehouse.gov/articles/final-modernization-report/ ; Report to the President on Federal IT Moderization, *available at* https://itmodernization.cio.gov/.

[87] Executive Order, at 5.

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

[89] *Id.* at 6.

[90] *Id.*

[91] *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* , National Telecommunications and Information Administrations, U.S. Dep't of Commerce, Jan. 5, 2018, *available at* https://www.ntia.doc.gov/report/2018/report-president-enhancing-resilience-internet-and-communications-ecosystem-against .

[92] *Id.* at 6-7.

[93] *Id.* at 7.

[94] *Id.*

[95] *Id.*

[96] *Id.* at 7-8.

[97] *Id.* at 8-9.

[98] Lily Hay Newman, *Taking Stock of Trump's Cybersecurity Executive Order so Far* , WIRED, Sept. 3, 2017, *available at* https://www.wired.com/story/trump-cybersecurity-executive-order/.

[99] See, e.g., Sonam Sheth, *Over a Quarter of the Members on Trump's Cybersecurity Advisory Council Have Resigned En Masse* , Business Insider, Aug. 28, 2017, *available at* http://www.businessinsider.com/members-of-trump-cybersecurity-council-resign-2017-8.

[100] Joseph Marks, *Trump Administration Plans a New Cybersecurity Strategy*, Defense One, Oct. 25, 2017, *available at* http://www.defenseone.com/technology/2017/10/trump-administration-plans-new-cybersecurity-strategy/142042/.

[101] Vulnerabilities Equities Policy and Process for the United States Government, Nov. 15, 2017, *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[102] *Id.* at 1.

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

[104] *Id.* at 6-7.

[105] *Id.*

[106] *Id.* at 7-8.

[107] *Id.* at 13-14.

[108] David Shepardson, *Trump Signs Repeal of U.S. Broadband Privacy Rules*, Reuters, Apr. 3, 2017, https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR.

[109] Richard Lawler, *Trump Signs Bill Rolling Back FCC Privacy Rules for ISPs*, Engadget, Apr. 3, 2017, https://www.engadget.com/2017/04/03/trump-signs-bill-rolling-back-fcc-privacy-rules-for-isps/.

[110] *Id.*

[111] *Shepardson* , supra note 109.

[112] *See generally* 50 U.S.C. § 1881 (2012).

[113] *See, e.g.* , 50 U.S.C. § 1881a.

[114] *The FISA Amendments Act: Q &A* , Office of the Director of National Intelligence, https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf.

[115] H.R. 139, 115th Cong. (2017).

[116] S. 2010, 115th Cong. (2017); *see also* David Shortell, *Senate Intel Advances Bill to Reauthorize Spying Program with Minimal Reform* , CNN, Oct. 27, 2017, http://www.cnn.com/2017/10/26/politics/fisa-702-reauthorization-bill-advanced/index.html.

[117] Pub. L. 115-96 (2017); *see also* Matthew Kahn, *Congress Buys Itself Another Three Weeks on Section 702*, Lawfare, Dec. 22, 2017, https://www.lawfareblog.com/year-review-fisa-section-702.

[118] H. 137, 115th Cong. (2017); *see also* Charlie Savage, Eileen Sullivan & Nicholas Fandos, *House Extends Surveillance Law, Rejecting New Privacy Safeguards* , N.Y. T IMES, Jan. 11, 2018, https://www.nytimes.com/2018/01/11/us/politics/fisa-surveillance-congress-trump.html.

[119] *See* Ted Barrett and Ashley Killough, *Senate Passes FISA Section 702 Reauthorization*, CNN Politics, Jan. 18, 2018, http://www.cnn.com/2018/01/18/politics/fisa-reauthorization-senate-vote/index.html.

[120] *See* Gregory Korte and Erin Kelly, *Trump signs bill extending surveillance law – the same law he says was used to spy on him* , USA Today, Jan. 19, 2018, https://www.usatoday.com/story/news/politics/onpolitics/2018/01/19/trump-signs-bill-extending-surveillance-law-same-law-he-says-used-spy-him/1049663001/.

[121] *See* Andrew Liptak, *President Donald Trump Has Signed the FISA Reauthorization Bill* , The Verge, Jan. 20, 2018, https://www.theverge.com/2018/1/20/16913534/president-donald-trump-signed-fisa-amendments-reauthorization-act-of-2017-section-702.

[122] *See* 18 U.S.C. § 2510 (2012).

[123] H.R. 387, 115th Cong. (2015).

[124] Mario Trujillo, *House Unanimously Passes Email Privacy Bill*, The Hill, Apr. 27, 2016, http://thehill.com/policy/technology/277897-house-unanimously-passes-bill-to-protect-email-privacy.

[125] S. 1654, 115th Cong. (2017).

[126] H.R. 1616, 115th Cong. (2017); *see also* Michael Macagnone, *House Authorizes National Cyber Security Center*, Law360, May 16, 2017, https://www.law360.com/privacy/articles/924495.

[127] Pub. L. No. 115-76 (2017).

[128] H.R. 4081, 115th Cong. (2017); S. 2124, 115th Cong. (2017).

[129] Mike Lennon, *U.S. Senators Introduce SEC Cybersecurity Disclosure Legislation* , Security Week, Dec. 18, 2015, http://www.securityweek.com/us-senators-introduce-sec-cybersecurity-disclosure-legislation.

[130] *See Security Breach Notification Laws* , National Conference of State Legislatures, Jan. 4, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-

notification-laws.aspx (listing the 47 states, along with the District of Columbia, Guam, Puerto Rico, and the Virgin Islands that have passed data breach notification laws).

[131] *See* Nat'l Conference of State Legislatures, Cybersecurity Legislation 2017, http://ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx (last visited Jan. 22, 2018).

[132] *See* Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (2017) (disapproving Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report and Order, 81 Fed. Reg. 87,274 (Dec. 2, 2016)).

[133] *See* California Consumer Privacy Act of 2018, Initiative No. 17-0027 (Cal. 2018), *available at* https://oag.ca.gov/system/files/initiatives/pdfs/17-0027%20%28Consumer%20Privacy%29_1.pdf .

[134] Data Breach Notification Act, H.B. 15 (N.M. 2017), *available at* https://legiscan.com/NM/text/HB15/2017 (defining "personal identifying information" as an "[i]ndividual's first name or last initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable: social security number; driver's license number; government issued identification number; account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account; or biometric data").

[135] Act to Amend Title 6 of the Delaware Code Relating to Breaches of Security Involving Personal Information, H.B. 180 (Del. 2017), *available at* https://legis.delaware.gov/BillDetail/26009.

[136] H.J.R. 59, 100th Gen. Assemb., 1st Sess. (Ill. 2017), *available at* http://ilga.gov/legislation/fulltext.asp?DocName=10000HJ0059eng&GA=100&SessionId=91&DocTypeId=HJR&LegID=107003&DocNum=59&GAID=14&Session=&print=true.

[137] *See* Nat'l Conference of State Legislatures, Cybersecurity Legislation 2017, http://ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx (last visited Jan. 22, 2018) (discussing H.R. 353 (P.R. 2017)); *see also* H.R. 353 (P.R. 2017), *available at* http://www.oslpr.org/2017-2020/%7B89C0F2C716C0425EA321DE9FC40CC10A%7D.docx (Spanish-language version).

[138] H.B. 7304 (Conn. 2017), *available at* https://www.cga.ct.gov/2017/act/pa/pdf/2017PA-00223-R00HB-07304-PA.pdf.

[139] S.B. 33, 64th Legis. Sess. (Wy. 2017), *available at* https://legiscan.com/WY/text/SF0033/2017.

[140] S.B. 1028, 217th Leg. (N.J. 2017), *available at* https://legiscan.com/NJ/text/S1028/2016.

[141] Assemb. B. 2765 (N.Y. 2017), *available at* http://assembly.state.ny.us/leg/?default_fld=&bn=A02765&term=2017&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y.

[142] S.B. 2406-A (N.Y. 2017), *available at* http://legislation.nysenate.gov/pdf/bills/2017/S2406A.

[143] Colo. Rev. Stat. Ann. § 24-72-204.5 (West 2017); Tenn. Code. Ann. § 10-7-512 (West 2017).

[144] Conn. Gen. Stat. Ann. § 31-48d (West 2017); Del. Code Ann. tit. 19, § 705 (West 2017).

[145] Conn. Gen. Stat. Ann. § 31-48d(c).

[146] Del. Code Ann. tit. 19, § 705(c).

[147] H.B. 2371, 100th Gen. Assemb., 1st Sess. (Ill. 2017), *available at* http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=91&GA=100&DocTypeId=HB&DocNum=2371&GAID=14&LegID=103007&SpecSess=&Session=.

[148] Assemb. B. 4936, 217th Leg. (N.J. 2017), *available at* https://legiscan.com/NJ/text/A4936/2016; H.B. 3221, 79th Legis. Sess. (Or. 2017), *available at* https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/HB3221.

[149] Assemb. B. 276 (Cal. 2017), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB276.

[150] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[151] *Id.* at 1545.

[152] *Id*.

[153] *In re Horizon Healthcare Servs. Inc. Data Breach Litig* ., 846 F.3d 625, 634–35 (3d Cir. 2017).

[154] *Id*. at 634–35.

[155] *Id*. at 640 (footnotes omitted); *see also id*. ("There is thus a *de facto* injury that satisfies the concreteness requirement for Article III standing.") (footnote omitted).

[156] *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017).

[157] *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017).

[158] *Id*.

[159] *Beck v. McDonald*, 848 F.3d 262, 274–75 (4th Cir.), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307 (2017).

[160] *See e.g.*, *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, No. MC 15-1394 (ABJ), 2017 WL 4129193, at *34–35 (D.D.C. Sept. 19, 2017) ("Neither complaint directly alleges, or marshals any facts that would support an inference, that those behind this attack are likely to use the information for credit card fraud or identify theft purposes, that they are likely to make it available to other criminals for that purpose, or that the breach has enabled other bad actors to have greater access to the information than they did before."), *appeals docketed*, No. 17-5217 (D.C. Cir. Sep. 27, 2017), No. 17-5232 (D.C. Cir. Oct. 12 2017), No. 18-1182 (Fed. Cir. Nov. 15, 2017); *In re VTech Data Breach Litig.*, No. 15 CV 10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017) ("Plaintiffs here fail to make the connection between the data breach they allege and the identity theft they fear. Specifically, plaintiffs do not explain how the stolen data would be used to perpetrate identity theft."); *Nayab v. Capital One Bank, N.A.*, No. 3:16-CV-3111-CAB-MDD, 2017 WL 2721982, at *2–3 (S.D. Cal. June 23, 2017) (finding that allegations of "increased risk" of identity theft were "speculative and conjectural"), *appeal docketed*, No. 17-55944 (9th Cir. July 5, 2017).

[161] *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017).

[162] *Id.* at 765–67 .

[163] *Id.* at 769 (citing *Attias*, 865 at 625–29; *Whalen*, 689 F. App'x at 89–91;*Beck*, 848 F.3d at 273–76; *Galaria v. Nationwide Mut. Ins.*, 663 F. App'x. 384, 387–90 (6th Cir. 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966–69 (7th Cir. 2016); and *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692–93 (7th Cir. 2015)).

[164] *Id.* at 769, 771 (citation omitted).

[165] *Id.* at 772–74.

[166] *See Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1117 (9th Cir. 2017), *petition for cert. filed*, No. 17-806 (U.S. Dec. 6, 2017).

[167] *Id.*

[168] *Syed v. M-I, LLC*, 853 F.3d 492, 499–500 (9th Cir. 2017), *cert. denied*, No. 16-1524, 2017 WL 2671483 (U.S. Nov. 13, 2017).

[169] *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017).

[170] *Id.*

[171] *See Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1340–41 (11th Cir. 2017) ("We conclude that violation of the VPPA constitutes a concrete harm. . . . The structure and purpose of the VPPA supports the conclusion that it provides actionable rights.") (citations omitted).

[172] *See e.g.*, *Aguirre v. Absolute Resolutions Corp.*, No. 15 C 11111, 2017 WL 4280957, at *5 (N.D. Ill. Sept. 27, 2017) (FDCPA case); *Hargrett v. Amazon.com DEDC LLC*, 235 F. Supp. 3d 1320, 1326

(M.D. Fla. 2017) (FCRA case); *Bock v. Pressler & Pressler, LLP*, 254 F. Supp. 3d 724, 734–737 (D.N.J. 2017) (FDCPA case).

[173] *See Groshek v. Time Warner, Inc.*, 865 F.3d 884, 887 (7th Cir. 2017).

[174] *Id*. at 889.

[175] *Dreher v. Experian Info. Sols., Inc.*, 856 F.3d 337, 346–47 (4th Cir. 2017).

[176] *See id*. at 347.

[177] *See Crupar-Weinmann v. Paris Baguette Am., Inc.*, 861 F.3d 76, 81–82 (2d Cir. 2017); *Katz v. Donna Karan Co., L.L.C.*, 872 F.3d 114, 121 (2d Cir. 2017) ("FACTA does not prohibit printing the [credit card] issuer identity on a receipt . . . .").

[178] *See e.g., Fullwood v. Wolfgang's Steakhouse, Inc.*, No. 13 CIV. 7174 (KPF), 2017 WL 5157466, at *5–6 (S.D.N.Y. Nov. 3, 2017); *Kamal v. J. Crew Grp., Inc.*, No. CV 2:15-0190 (WJM), 2017 WL 2443062, at *4–5 (D.N.J. June 6, 2017).

[179] *See Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 913 (7th Cir. 2017).

[180] *Id*. at 910.

[181] *See Santana v. Take-Two Interactive Software, Inc.*, --- F. App'x ----, 2017 WL 5592589, at *5 (2d Cir. Nov. 21, 2017).

[182] *Id*. at *2–3.

[183] *See Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 1005 (N.D. Cal. 2017) (holding that the plaintiff alleged an adequate injury based on allegation that the "[d]efendants captured and listened to private conversations without her knowledge or consent").

[184] *See In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1215–17 (C.D. Cal. 2017).

[185] *E.g., Whitaker v. Appriss, Inc.*, 229 F. Supp. 3d 809, 812–17 (N.D. Ind. 2017); *Hatch v. Demayo*, No. 1:16CV925, 2017 WL 4357447, at *3–6 (M.D.N.C. Sept. 29, 2017).

[186] *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017).

[187] *See Leyse v. Lifetime Entm't Servs., LLC*, 679 F. App'x 44, 46 (2d Cir. 2017); *Susinno v. Work Out World Inc.*, 862 F.3d 346, 352 (3d Cir. 2017).

[188] *See e.g., Melito v. Am. Eagle Outfitters, Inc.*, No. 14-CV-2440 (VEC), 2017 WL 3995619, at *7 (S.D.N.Y. Sept. 11, 2017) (certifying class and approving class settlement over objections, and holding that the "receipt of an unconsented to voicemail message was sufficient to establish a concrete injury"),*appeal docketed*, No. 17-3277 (2d Cir. Oct 10, 2017); *Heather McCombs, D.P.M., L.L.C. v.*

Cayan LLC, No. 15 C 10843, 2017 WL 1022013, at *4 (N.D. Ill. Mar. 16, 2017) (holding "that in pleading the receipt of an unsolicited fax advertisement in violation of the TCPA, Plaintiff has alleged a particularized and concrete injury sufficient to satisfy Article III"), *appeal dismissed*, No. 17-1946, 2017 WL 5185363 (7th Cir. July 7, 2017).

[189] *Legg v. PTZ Ins. Agency, Ltd.*, 321 F.R.D. 572, 577–78 (N.D. Ill. 2017), *appeal docketed*, No. 17-8018 (7th Cir. Aug. 31, 2017).

[190] Allison Grande,*Spokeo Wants Justices To Revisit Last Year' s Standing Ruling*, Law360 (Dec. 13, 2017, 10:50 PM), https://www.law360.com/cybersecurity-privacy/articles/994507/spokeo-wants-justices-to-revisit-last-year-s-standing-ruling.

[191] Allison Grande, *Spokeo Standing Fight Won't Go Another Round At High Court* , Law360 (Jan. 22, 2018, 4:15 PM), https://www.law360.com/cybersecurity-privacy/articles/1004192/spokeo-standing-fight-won-t-go-another-round-at-high-court.

[192] Michael Riley, Jordan Robertson, and Anita Sharpe, *The Equifax data breach has the hallmarks of state-sponsored pros* , Bloomberg Businessweek (Sept. 29, 2017), https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

[193] *See, e.g.*, Compl., *Allen et al v. Equifax, Inc.*, No. 1:17-cv-04544 (N.D. Ga. Nov. 10, 2017); *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 .

[194] *Id*.

[195] *See* Compl., *People of the State of California v. Equifax, Inc.*, No. CGC-17-561529 (Sep. 26, 2017); Compl., *City of Chicago v. Equifax, Inc.*, 2017-CH-13047 (Sep. 28, 2017).

[196] Compl., *Commonwealth of Massachusetts v. Equifax, Inc.*, No. 1784CV03009 (Sep. 19, 2017).

[197] Renae Merle, *After the breach, Equifax now faces the lawsuits*, Washington Post (Sep. 22, 2017), https://www.washingtonpost.com/news/business/wp/2017/09/22/after-the-breach-equifax-now-faces-the-lawsuits/?utm_term=.185a237742fb .

[198] Compl., *Kuhns et al. v. Equifax, Inc.*, No. 1:17-cv-03463 (N.D. Ga. Sep. 8, 2017).

[199] *See, e.g.*, *Knepper v. Equifax Information Servs.*, LLC., No. 2:17-CV-02368 (D. Nev. Oct. 2, 2017) (order granting motion to stay pending consolidation).

[200] *In re Equifax, Inc. Customer Data Security Breach Litigation* , MDL No. 2800 (J.P.M.L. Dec. 6, 2017).

[201] Teri Robinson, *Open AWS S3 bucket exposes sensitive Experian and census info on 123 million U.S. households* , SC Magazine (Dec. 20, 2017), https://www.scmagazine.com/open-aws-s3-bucket-exposes-sensitive-experian-and-census-info-on-123-million-us-households/article/720067/ .

[202] *Id*.

[203] *Id*.

[204] Ray Schultz, *Alteryx Slammed with Two Data Breach Suits*, Email Marketing Daily (Dec. 22, 2017), https://www.mediapost.com/publications/article/312126/alteryx-slammed-with-two-data-breach-suits.html.

[205] *Elec. Privacy Info. Ctr. v. FBI* , No. 1:17-cv-00121 (D.D.C. Jan. 18, 2017).

[206] Compl., *Microsoft Corp. v. Does 1-12*, No.2016-cv-00993 (E.D. Va. Filed Aug. 3, 2016), at ECF No. 1; *see also* Kevin Poulsen, *Putin's Hackers Now Under Attack – From Microsoft*, Daily Beast (July 20, 2017), https://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network .

[207] Selena Larson, *Data of almost 200 million voters leaked online by GOP analytics firm* , CNN (June 19, 2017), http://money.cnn.com/2017/06/19/technology/voter-data-leaked-online-gop/index.html?iid=EL .

[208] *Id* .

[209] Compl., *McAleer et al v. Deep Root Analytics*, LLC, No. 6:17-cv-01142 (M.D. Fl. June 21, 2017).

[210] Order, *McAleer et al v. Deep Root Analytics*, LLC, No. 6:17-cv-01142 (M.D. Fl. Nov. 7, 2017).

[211] Callum Borchers, *What we know about the 21 states targeted by Russian hackers* , Washington Post (Sept. 23, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.28d2dcb475c7 .

[212] *Id.*

[213] *See, e.g.* , Compl., *Weiss et al. v. Arby's Restaurant Group, Inc.*, No. 1:17-cv-01035 (N.D. Ga., Mar. 22, 2017).

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

[215] *See, e.g.* , Order, *In re Sonic Corp. Customer Data Security Breach Litig.*, No. 2807 (JPML, Dec. 15, 2017); David P. Willis, *Sonic Drive-In hit by security breach*, Asbury Park Press (Sept. 27, 2017), https://www.usatoday.com/story/tech/2017/09/27/sonic-drive-hit-security-breach/708850001/ .

[216] Josh Magness & Donovan Harrell, *Pizza Hut was hacked, company says*, Miami Herald (Oct. 14, 2017, updated Oct. 18, 2017), https://www.usatoday.com/story/tech/2017/09/27/sonic-drive-hit-security-breach/708850001/ .

[217] Compl., *Yoachim et al. v. Pizza Hut Inc.*, No. 17-cv-1675 (W.D. Wash., Nov. 7, 2017).

[218] Jamie Biesiada, *Sabre sued for data breach of hotel res system*, Travel Weekly (July 14, 2017), http://www.travelweekly.com/Travel-News/Travel-Technology/Sabre-sued-for-data-breach-of-hotel-res-system .

[219] Compl., *Orr v. InterContinental Hotels Group, PLC*, No. 1:17-cv-01622 (N.D. Ga., May 5, 2017).

[220] Compl., *Banus v. Whole Foods Market Group, Inc.*, No. 1:17-cv-02132 (N.D. Ohio, Oct. 10, 2017).

[221] *Largest Healthcare Data Breaches of 2017*, HIPAA J. (Jan. 4, 2018), https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/.

[222] *Id.*

[223] Marianne Kolbasuk McGee, *Breach involving encrypted devices raises questions*, Health Care Info Security (Mar. 23, 2017), https://www.healthcareinfosecurity.com/breach-involving-encrypted-devices-raises-questions-a-9789 .

[224] *Largest Healthcare Data Breaches of 2017*, HIPAA J. (Jan. 4, 2018), https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/.

[225] Compl., *Palmer v. Bowling Green-Warren Cnty. Comm. Hosp. Corp.*, No. 17-CI-00579 (Cir. Ct. Warren Cnty., May 12, 2017).

[226] Jeff John Roberts, *Law firm DLA Piper reels under cyber attack, fate of files unclear* , Fortune (June 29, 2017), https://www.healthcareinfosecurity.com/breach-involving-encrypted-devices-raises-questions-a-9789 .

[227] *Guardian to fight legal action over Paradise Papers* , The Guardian (Dec. 18, 2017), https://www.theguardian.com/uk-news/2017/dec/18/guardian-bbc-legal-action-paradise-papers?CMP=Share_iOSApp_Other .

[228] *Id* .

[229] *Id* .

[230] *See* Order, In re: *Yahoo! Inc. Customer Data Sec. Breach Litigation*, No. 16-MD-02752-LHK, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017).

[231] *Id.* at *17.

[232] *Id* . at *53.

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

[234] *Id* . at 20, 28.

[235] *Id* . at 36-38.

[236] *Id* . at 39-47, 49-50.

[237] In re *VTech Data Breach Litig.*, No. 1:15-cv-10889, -10891, -11620, -11885, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017).

[238] *Id* .

[239] Amended Complaint, In re *VTech Data Breach Litig.*, No. 1:15-cv-10889, -10891, -11620, -11885 (N.D. Ill. Aug. 17, 2017).

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

[241] *Id.* at 14.

[242] *Id.* at 12.

[243] *SELCO Comm. Credit Union v. Noodles & Co.* , 267 F. Supp. 3d 1292 (D. Colo. 2017).

[244] *Id* .

[245] *Id* .

[246] *Attias v. CareFirst, Inc.* , 865 F.3d 620, 622-23 (D.C. Cir. 2017).

[247] *Id* . at 628.

[248] *Id* .

[249] *Beck v. McDonald* , 848 F.3d 262, 267 (4th Cir. Feb. 6, 2017).

[250] *Id* . at 274, 276-77.

[251] *Id* . at 275.

[252] *Attias* , 865 F.3d at 628.

[253] *Beck* , 848 F.3d at 275.

[254] *Whalen v. Michaels Stores, Inc.* , 689 Fed. App'x 89, 90-91 (2d Cir. 2017).

[255] *See* Alison Frankel, *8th Circuit Adds to Data Breach Litigation Uncertainty, Ahead of SCOTUS Petition* , Reuters (Sept. 1, 2017), https://www.reuters.com/article/us-otc-databreach/8th-circuit-adds-to-data-breach-litigation-uncertainty-ahead-of-scotus-petition-idUSKCN1BC5OJ.

[256] In re *SuperValu, Inc., Customer Data Sec. Breach Litig.*, 870 F.3d 763, 770-72 (8th Cir. 2017).

[257] *Id.* at 772.

[258] Complaint, *Microsoft Corp. v. Does 1-12*, No. 2016-cv-00993 (E.D. Va. Aug. 3, 2016), ECF No. 1; *see also* Kevin Poulsen, *Putin's Hackers Now Under Attack – From Microsoft*, Daily Beast (July 20, 2017), https://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network.

[259] *Id* .

[260] Preliminary Injunction Order, *Microsoft Corp. v. Does 1-12* , No. 2016-cv-00993 (E.D. Va. Aug. 12, 2016), ECF No. 33.

[261] Motion for Default Judgment and Permanent Injunction, *Microsoft Corp. v. Does 1-12*, No. 2016-cv-00993 (E.D. Va. Jun. 29, 2017), ECF No. 55.

[262] *Guardian to Fight Legal Action over Paradise Papers* , The Guardian (Dec. 18, 2017), https://www.theguardian.com/uk-news/2017/dec/18/guardian-bbc-legal-action-paradise-papers.

[263] Settlement Agreement and Release at 11, In re *Anthem, Inc. Data Breach Litig.* ("In re *Anthem* "), No. 5:15-md-02617-LHK, (N.D. Cal. June 23, 2017).

[264] *See* In re *Anthem*, 162 F. Supp. 3d 953, 967 (N.D. Cal. 2016).

[265] *See id.* at 968.

[266] *Id.* at 1016.

[267] Settlement Agreement and Release at 4, *In re Anthem*, No. 5:15-md-02617-LHK (N D. Cal. June 23, 2017).

[268] *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).

[269] Settlement Agreement and Release at 11, *In re Anthem*, No. 5:15-md-02617-LHK, (N.D. Cal. May 31, 2017).

[270] *Id.*

[271] *Id.* at 11, 23.

[272] *Id.* at 10.

[273] *See* Memorandum of Law in Support of Consumer Plaintiffs' Motion for Preliminary Approval of Class Settlement, In re: *The Home Depot, Inc., Customer Data Sec. Breach Litig.* ("In re *Home Depot*"), No. 1:14-md-02583-TWT (N.D. Ga. Aug. 23, 2016).

[274] *See* Final Order and Judgment at 1–2, In re *Home Depot*, No. 1:14-md-02583-TWT (N.D. Ga. Sept. 22, 2017).

[275] *Id.* at 3.

[276] *Id.* at 13.

[277] *See* Memorandum and Order at 3, In re: *Target Corp. Customer Data Sec. Breach Litig.*, No. 14-md-2522 (PAM) (D. Minn. May 17, 2017).

[278] *See id.*

[279] *See id.* at 19-21.

[280] *See generally* Objector Olson's Amended Notice of Appeal, In re: *Target Corp. Customer Data Sec. Breach Litig.*, No. 14-md-2522 (PAM) (D. Minn. June 2, 2017).

[281] Press Release, N.Y. State Office of the Attorney Gen., A.G. Schneiderman Announces $18.5 Million Multi-State Settlement with Target Corporation over 2013 Data Breach (May 23, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over.

[282] *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 (adopting Settlement Agreement, ECF No. 327-3).

[283] *See* Settlement Agreement and Release at 10–18, 23, *In re Anthem*, No. 5:15-md-02617-LHK, (N.D. Cal. Jun. 23, 2017), ECF No. 869-8.

[284] 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).

[285] 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).

[286] 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.

[287] 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.

[288] *St. Joseph Health System Med. Info. Cases* , JCCP No. 4716 (Cal. Sup. Ct.).

[289] 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).

[290] 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).

[291] 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.

[292] 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.

[293] Opinion at 3, 9–11, *Palkon et al. v. Holmes et al*., No. 2:14-cv-01234 (SRC) (D.N.J. Oct. 20, 2014), ECF No. 49.

[294] Order Granting Motion to Dismiss, *In re Target Corp. S'holder Derivative Litig.*, No. 0:14-cv-00203 (PAM/JJK) (D. Minn. July 7, 2016), ECF No. 19; Target Corporation Report of the Special Litigation Committee at 2, *In re Target Corp. S'holder Derivative Litig.*, No. 0:14-cv-00203 (PAM/JJK) (Mar. 30, 2016), ECF No. 62-2; *see also* Memorandum of Law of the Special Litigation Committee of the Board of Directors of Target Corporation in Support of its Motion for Approval and Dismissal, *In re Target Corp. S'holder Derivative Litig.*, No. 0:14-cv-00203 (PAM/JJK) (D. Minn. May 6, 2016), ECF No. 59.

[295] Opinion and Order at 11, *In re The Home Depot, Inc. S'holder Derivative Litig.*, No. 1:15-cv-2999-TWT (N.D. Ga. Nov. 30, 2016), ECF No. 62.

[296] Unopposed Motion for Order for Preliminary Approval of Shareholder Derivative Settlement with Brief In Support, *In re The Home Depot, Inc. S'holder Derivative Litig.*, No. 1:15-cv-2999-TWT (N.D. Ga. Apr. 28, 2017), ECF No. 73; Notice of Proposed Settlement at 5, In re The Home Depot, Inc. S'holder Derivative Litig., No. 1:15-cv-2999-TWT (N.D. Ga. Apr. 28, 2017), ECF No. 74-4.

[297] Notice of Proposed Settlement at 4-5, *In re The Home Depot, Inc. S'holder Derivative Litig.*, No. 1:15-cv-2999-TWT (N.D. Ga. Apr. 28, 2017), ECF No. 74-4.

[298] *See* Updates Related to Investigation of Unusual Payment Card Activity at Wendy's, WENDYS.COM, (last visited Jan. 21, 2018), https://www.wendys.com/en-us/about-wendys/the-wendys-company-updates.

[299] Verified Shareholder Derivative Complaint at 71-74, *Graham v. Peltz et al*, No. 1:16-cv-01153-TSB (S.D. Ohio Dec. 16, 2016), ECF No. 1.

[300] *Id.* at 4.

[301] Memorandum in Support of Defendants' Motion to Dismiss Verified Shareholder Derivative Complaint, *Graham v. Peltz et al*, No. 1:16-cv-01153-TSB (S.D. Ohio Mar. 10, 2017), ECF No. 9-1.

[302] *Id.* at 15.

[303] Complaint, *In re: Yahoo! Inc. Shareholder Derivative Litigation*, No. 5:17-cv-00787-LHK (N.D. Cal. Feb. 16, 2017), ECF No. 1.

[304] Complaint, *Okla. Firefighters Pension And Ret. Sys. v. Brandt, et al.* , No. 2017-0133-SG, 2017 WL 771182 (Del. Ch. Feb. 23, 2017).

[305] Order Staying Case Pending Entry of Final Judgments in Securities and Customer Class Actions, *In re: Yahoo! Inc. Shareholder Derivative Litigation*, No. 5:17-cv-00787-LHK (N.D. Cal. Sep. 25, 2017), ECF No. 40.

[306] Order Denying Motion to Dismiss, *Matera v. Google, Inc.*, No. 5:15-cv-04062-LHK (N.D. Cal. Aug. 12, 2016), ECF No. 49.

[307] *Matera v. Google Inc.*, No. 15-CV-04062, 2016 WL 5339806, at *14 (N.D. Cal. Sept. 23, 2016).

[308] *Id.*

[309] *Id.* at *16 ("[I]t appears that there is no 'real and immediate threat of repeated injury in the future.'").

[310] Stipulation Staying Proceedings, *Matera v. Google, Inc.*, No. 5:15-cv-04062-LHK (N.D. Cal. Nov. 28, 2016), ECF No. 60.

[311] *Matera v. Google Inc.*, 2017 WL 1365021, at *2 (N.D. Cal. 2017).

[312] *Id.*

[313] Motion for Preliminary Approval of Class Action Settlement, *Matera v. Google, Inc.*, No. 5:15-cv-04062-LHK (N.D. Cal. Dec. 13, 2016), ECF No. 62.

[314] *Id.*

[315] *Id.*

[316] *Id.*

[317] Motion for Preliminary Approval of Class Action Settlement, *Matera v. Google, Inc.*, 5:15-cv-04062-LHK (N.D. Cal. July 21, 2017), ECF No. 79.

[318] *Id.*

[319] Order Granting Preliminary Approval of Class Action Settlement, *Matera v. Google, Inc.*, 5:15-cv-04062-LHK (N.D. Cal. Aug. 31, 2017), ECF No. 89.

[320] Amended Complaint, *Cooper & Parikh v. Slice Technologies, Inc., & UnrollMe Inc.* , No. 1:17-cv-07102-JPO (N.D. Cal. July 10, 2017), ECF No. 29.

[321] *Id.*

[322] *Id.*

[323] Motion to Dismiss, *Cooper & Parikh v. Slice Technologies, Inc., & UnrollMe Inc.* , No. 1:17-cv-07102-JPO (N.D. Cal. Oct. 12, 2017), ECF No. 54.

[324] 18 U.S.C. § 2511(2)(d).

[325] *See* Ala. Code §§ 13A-11-30(1), 31; Alaska Stat. Ann. §§ 42.20.300(a), 310(a)(1); Ariz. Rev. Stat. Ann. §§ 13-3012(5(c)), (9); Ark. Code Ann. § 5-60-120; Colo. Rev. Stat. Ann. § 18-9-303(1); Conn. Gen. Stat. Ann. §§ 53a-187, -189 *but see* § 52-570d; D.C. Code Ann. § 23-542(b)(3); Ga. Code Ann. §§ 16-11-62, 66(a); Haw. Rev. Stat. Ann. § 803-42(3)(A); Idaho Code Ann. § 18-6702(2)(d); Ind. Code Ann. § 35-31.5-2-176; Iowa Code Ann. §§ 727.8, 808B.2 (2)(c); Kan. Stat. Ann. § 21-6101; Ky. Rev. Stat. Ann. §§ 526.010, 526.020; La. Stat. Ann. § 15:1303(c)(4); Me. Stat. tit. 15, § 710; Mich. Comp. Laws § 750.539(c) *but see Sullivan v. Gray*, 324 N.W.2d 58 (Mich. Ct. Ap.. 1982); Minn. Stat. Ann. § 626A.02(d); Miss. Code. Ann. § 41-29-531(e); Mo. Ann. Stat. § 542.402(2)(3); Neb. Rev. Stat. Ann. §§ 86-276, -290(2)(c); N.J. Stat. Ann. §§ 2A:156A-2, -4(d); N.M. Stat. Ann. § 30-12-1(C); N.Y. Penal Law §§ 250.00(1), 250.05; N.C. Gen. Stat. Ann. § 15A-287(a); N.D. Cent. Code Ann. § 12.1-15-02; Ohio Rev. Code Ann. §§ 2933.51, 2933.52(B)(4); Okla. Stat. tit. 13, §§ 176.2, 176.4; Or. Rev. Stat. Ann. §§ 165.535, 165.540; R.I. Gen. Laws Ann. §§ 11-35-21, 12-5.1-1; S.C. Code Ann. §§ 17-30-15, -30; S.D. Codified Laws §§ 23A-35A-1, -20; Tenn. Code Ann. §§ 39-13-601, -604, 40-6-303; Tex. Penal Code Ann. § 16.02; Tex. Code Crim. Proc. Ann. art. 18.20; Utah Code Ann. § 77-23a-3, -4; Va. Code

Ann. § 19.2-62; W. Va. Code Ann. § 62-1D-3; Wis. Stat. Ann. §§ 968.27, 968.31 *but see* Wis. Stat. Ann. § 885.365(1) (rendering inadmissible as evidence in civil cases recordings obtained without the consent of all parties); Wyo. Stat. Ann. § 7-3-702. Vermont has no applicable statute or definitive cases on consent to record a phone conversation.

[326] Cal. Penal Code § 632; Del. Code Ann. tit. 11, § 1335(a)(4) *but see* § 2402(c)(4); Fla. Stat. § 934.03(3)(d); 720 Ill .Comp. Stat. 5/14-2(a); Md. Code Ann., Cts. & Jud. Proc. § 10-402(c)(3); Mass. Gen. Laws Ann. ch. 272, § 99; Mont. Code Ann. § 45-8-213; Nev. Rev. Stat. Ann. §§ 200.620, 200.650 *but see Lane v. Allstate Ins. Co.*, 969 P.2d 938 (Nev. 1998); N.H. Rev. Stat. Ann. § 570-A:2(I-a); 18 Pa. Stat. and Cons. Stat. Ann. §§ 5702, 5704; Wash. Rev. Code Ann. § 9.73.030.

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

[328] *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).

[329] Complaint, *Wang, et al. v. Wells Fargo Bank, N.A., et al.*, 1:16-CV-11223 (N.D. Ill. Dec. 9, 2017), ECF No. 1.

[330] *Brinkley v. Monterey Fin. Servs., Inc.* , 873 F.3d 1118, 1122-23 (9th Cir. 2017).

[331] 28 U.S.C. § 1332(d)(4)(B).

[332] *Brinkley* , 873 F.3d at 1121-23.

[333] *Id.*

[334] *Raffin v. Medicredit, Inc.* , No. 15-CV-4912, 2017 WL 131745 (C.D. Cal. Jan. 3, 2017).

[335] *Id.* at *1. § 632 prohibits recordings over landlines.

[336] *Id.* at *3.

[337] *Id.* at *8.

[338] *See, e.g.* , *Zaklit v. Nationstar Mortg. LLC*, 5:15-CV-2190-CAs, 2017 WL 3174901 (C.D. Cal. July 24, 2017); *Ronquillo-Griffin v. Telus Commc'ns, Inc.*, No. 17-CV-129-JM, 2017 WL 2779329 (S.D. Cal. June 27, 2017).

[339] *Compare Raffin*, 2017 WL 131745, at *3 *with Saulsberry v. Meridian Fin. Servs., Inc.*, No. 14-CV-6256, 2016 WL 3456939, at *15-16 (C.D. Cal. Apr. 14, 2016).

[340] *See Raffin*, 2017 WL 131745; *Zaklit*, 2017 WL 3174901; *Reyes v. Educational Credit Mgmt. Corp.*, No. 15-CV-00628, 2017 WL 4169720 (S.D. Cal. Sept. 20, 2017).

[341] *See Ronquillo Griffin* , 2017 WL 2779329, at *3-4; *Carrese*, 2016 WL 6069198, at *8 n.8 (collecting cases); *but see Granina v. Eddie Bauer LLC*, No. BC569111, 2015 WL 9855304 (L.A. Cty. Super. Ct. Dec. 2, 2015).

[342] *People v. Guzman* , 217 Cal. Rptr. 3d 509 (Cal. Ct. App. 2017).

[343] Cal. Const., art. I, § 28, subd. (f), ¶ (2).

[344] *Guzman* , 217 Cal. Rptr. 3d at 514-19.

[345] *State v. Smith* , No. 1 CA-CR 16-0259 PRPC, 2017 WL 3481244 (Ariz. Ct. App. Aug. 15, 2017).

[346] *Id.* at *4.

[347] *State v. Smith* , 405 P.3d 997 (Wash. 2017).

[348] *Id.* at 1001.

[349] Class Action Settlement Agreement, *Opperman et al v. Kong Technologies, Inc. et al.*, No. 3:13-cv-00453-JST (N.D. Cal, April 3, 2017), ECF No. 884.

[350] Complaint, *Opperman et al v. Kong Technologies, Inc. et al.*, No. 3:13-cv-00453-JST (W.D. Texas Mar. 12, 2012), ECF No. 1.

[351] Class Action Settlement Agreement, supra note 246.

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

[353] *In re Vizio, Inc., Consumer Privacy Litigation*, 238 F.Supp.3d 1204, 1228 (C.D. Cal. 2017).

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

[355] *Id.*

[356] Motion to Dismiss Second Consolidated Complaint and Motion to Strike Class Allegations, *In re Vizio, Inc., Consumer Privacy Litigation*, 8:16-ml-02693-JLS-KES (C.D. Cal April 13, 2017), ECF No. 145.

[357] Order Denying Defendants' Motion to Dismiss and Strike, *In re Vizio, Inc., Consumer Privacy Litigation*, 8:16-ml-02693-JLS-KES (C.D. Cal July 25, 2017), ECF No. 199.

[358] *Id.*

[359] *Id.*

[360] *Id.*

[361] Complaint, *Satchell v. Signal360, Inc. et al*, No. 4:16-cv-04961-JSW (N.D. Cal Aug. 29, 2017), ECF No. 1.

[362] *Satchell v. Sonic Notify, Inc.*, 234 F.Supp.3d 996 (N.D.Cal. 2017).

[363] *Id.* at 1005-1009.

[364] Amended Complaint, *Satchell v. Signal360, Inc. et al*, No. 4:16-cv-04961-JSW (N.D. Cal Mar. 13, 2017), ECF No. 58.

[365] Order Granting In Part and Denying In Part Motions to Dismiss, *Satchell v. Sonic Notify, Inc., et al.*, No. 4:16-cv-04961-JSW (N.D. Cal Nov. 20, 2017), ECF No. 89.

[366] *Id.* at 10.

[367] *Id.* at 10-12.

[368] Complaint, *Rackemann v. Lisnr, Inc. et al.*, No. 2:16-cv-01573-AJS (W.D. Penn. Oct. 16, 2016), ECF No. 1.

[369] *Rackemann v. LISNR, Inc.*, 2017 WL 4340349, at *5 (S.D. Ind. 2017).

[370] *Id.* at *5-8.

[371] *Id.* at *8.

[372] *Id.* at *8 (citing *Luis v. Zang*, 833 F.3d 619, 633 (6th Cir. 2016)).

[373] *Id.* at *9.

[374] Amended Complaint, *Zak v. Bose Corp.*, No. 1:17-cv-02928 (N.D. Ill. July 10, 2017), ECF No. 24.

[375] *Id.*

[376] *Id.*

[377] *Id.*

[378] Motion to Dismiss Plaintiffs' Second Amended Complaint, *Zak v. Bose Corp.*, No. 1:17-cv-02928 (N.D. Ill. Aug. 3, 2017), ECF No. 28.

[379] *Id.*

[380] Complaint, *Allen v. Quicken Loans Inc. & Navistone, Inc.*, No. 2:17-cv-12352-ES-MAH (D. N.J. Dec. 1, 2017), ECF No. 1.

[381] Complaint, *Cohen v. Casper Sleep Inc. & Navistone*, No. 1:17-cv-09325 (S.D.N.Y. Nov. 28, 2017), ECF No. 1; Complaint, *Cohen v. New Moosejaw, LLC & Navistone*, No. 1:17-cv-09391 (S.D.N.Y. Nov. 30, 2017), ECF No. 1.

[382] 47 U.S.C. §§ 227 *et seq.*

[383] *ACA International v. FCC, et al* , No. 15-1211 (D.C. Cir. filed July 10, 2015).

[384] Rules & Regs. Implementing the Tel. Consumer Prot. Act of 1991, 30 FCC Rcd. 7961, 7975–76 ¶ 19 (2015).

[385] *Id.* at 7989–90 ¶ 47.

[386] *Modernizing the Telephone Consumer Protection Act*: *Hearing Before the Subcomm. on Communications and Technology of the H. Comm. on Energy and Commerce,* 114th Cong. 8-9 (2016) (statement of Representative Anna Eshoo).

[387] *Id.* at 3-41 (statement of Subcommittee Chairman Greg Walden).

[388] 12 C.F.R. § 1002.16(b).

[389] Pet. for Declaratory Ruling of All About The Message, LLC, *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991* , CG Docket No. 20-278 (FCC Mar. 31, 2017).

[390] Eric Zorn, *Hang Up Now On The Idea Of 'Ringless Voicemail'* , Chi. Trib., June 2, 2017, http://www.chicagotribune.com/news/opinion/zorn/ct-ringless-voicemail-20170602-column.html ; Letter from Edward J. Markey et al., U.S. Senate, to Ajit Pai, Chairman of the FCC (June 14, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-345975A4.pdf.

[391] *What We Do* , About the FCC, https://www.fcc.gov/about-fcc/what-we-do (last visited Jan. 22, 2018).

[392] Organizational Charts of the Federal Communications Commission, Federal Communications Commission, https://www.fcc.gov/sites/default/files/fccorg-08112017.pdf ; Jim Puzzanghera, *Here Are The Five Officials Who Will Decide The Controversial Changes to Net Neutrality Rules* , L.A. Times (Nov. 22, 2017), http://www.latimes.com/business/la-fi-net-neutrality-fcc-20171122-htmlstory.html.

[393] *See, e.g.* , Ajit Pai, *The FCC Shouldn't Enable More TCPA Lawsuits*, The Daily Caller (June 16, 2015), http://dailycaller.com/2015/06/16/the-fcc-shouldnt-enable-more-tcpa-lawsuits/2/.

[394] *Yaakov v. FCC* , No. 14-1234 (D.C. Cir. Mar. 31, 2017); *Statement of FCC Chairman Ajit Pai*, FCC News (Mar. 31, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-344186A1.pdf .

[395] Dissenting Statement of Commissioner Pai, Re: *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991* , CG Docket No. 02-278, WC Docket No. 07-135 (FCC July 10, 2015).

[396] *Krakauer v. Dish Network LLC* , No. 1:14-333, 2017 WL 2242952 (M.D.N.C. Oct. 3, 2017).

[397] *Id.* at *12.

[398] *United States v. Dish Network LLC* , 256 F. Supp. 3d 810 (C.D. Ill. June 5, 2017).

[399] *Id.* at 991.

[400] *United States v. Dish Network LLC*, No. 09-3073-SEM-RSH (C.D. Ill. *notice of appeal filed* June 16, 2017).

[401] *Birchmeier v. Caribbean Cruise Line, Inc.* , No. 1:12-cv-04069 (N.D. Ill. Mar. 2, 2017).

[402] *Id.*

[403] *See* Andrea Peterson, *How a Failed Supreme Court Bid Is Still Causing Headaches For Hulu and Netflix*, Washington Post (Dec. 27, 2013), *available at* https://www.washingtonpost.com/news/the-switch/wp/2013/12/27/how-a-failed-supreme-court-bid-is-still-causing-headaches-for-hulu-and-netflix/.

[404] 18 U.S. § 2710(b)(1).

[405] *Eichenberger v. ESPN, Inc.* , 876 F.3d 979, 982(9th Cir. 2017).

[406] *In re Nickelodeon Consumer Privacy Litig.* , 827 F.3d 262, 272–75 (3d Cir. 2016); *Sterk v. Redbox Automated Retail, LLC*, 770 F.3d 618, 623 (7th Cir. 2014).

[407] *See, e.g.* , *Yershov v. Gannet Satellite Info. Network, Inc.*, 204 F. Supp. 3d 353, 358-61 (D. Mass. 2016); *Boelter v. Advance Magazine Publishers Inc.*, 210 F. Supp. 3d 579, 590 (S.D.N.Y. 2016); *Austin-Spearman v. AMC Network Entm't LLC*, 98 F. Supp. 3d 662, 666 (S.D.N.Y. 2015); *In re Hulu Privacy Litig.*, No. C 11-03764 LB, 2013 WL 6773794, at *5 (N.D. Cal. Dec. 20, 2013); *Ellis v. Cartoon Network, Inc.*, No. 1:14-CV-484-TWT, 2014 WL 5023535, at *2 (N.D. Ga. Oct. 8, 2014), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir. 2015).

[408] *Eichenberger* , 876 F.3d at 984.

[409] *Spokeo, Inc. v. Robins* , 136 S. Ct. 1540 (2016).

[410] *Eichenberger* , 876 F.3d at 983.

[411] *Perry v. Cable News* , 854 F.3d 1336, 1340-41 (11th Cir. 2017).

[412] 18 U.S.C. § 2710(a)(3).

[413] *Yershov v. Gannett Satellite Information Network Inc.* , 820 F.3d 482, 486 (1st Cir. 2016) (emphasis added).

[414] *Id.*

[415] *In re Nickelodeon Consumer Privacy Litig.* , 827 F.3d 262, 290 (3d Cir. 2016) (emphasis added).

[416] *Id.* at 284.

[417] *C.A.F. v. Viacom, Inc.* , 137 S.Ct. 624 (2017).

[418] *Eichenberger* , 876 F.3d at 985.

[419] *Id* .

[420] *Id* . at 986 (quoting *Yershov*, 820 F.3d at 486); *Nickelodeon Consumer Privacy Litig.*, 827 F.3d at 290.

[421] *In re Vizio, Inc. Consumer Privacy Litig.* , 238 F. Supp. 3d 1204, 1225 (C.D. Cal. 2017).

[422] *Id* . at 1224-25.

[423] *In re Vizio, Inc. Consumer Privacy Litig.* , Case No. 8:16-ml-02693-JLS-KES (C.D. Cal. October 13, 2017), Dkt no. 224.

[424] *Perry* , 854 F.3d at 1342.

[425] *Id.*

[426] *Vizio* , 238 F. Supp. 3d at 1223.

[427] *Id.* at 1221-22.

[428] Cal. Civ. Code § 1747.08.

[429] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[430] *Medellin v. IKEA U.S.A. W., Inc.*, 672 F. App'x 782, 783 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 220 (2017).

[431] *Id.* (citing *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016)).

[432] *IKEA U.S.A. W., Inc. v. Medellin*, 138 S. Ct. 220 (2017).

[433] *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317 (Ill. Ct. App. Dec. 21, 2017).

[434] H.R. 3388, 115th Cong. (2017), *available at* https://www.congress.gov/bill/115th-congress/house-bill/3388/text

[435] *Id* ., at § 30130(a)(1)(A).

[436] Press Release, U.S. Senate Committee on Commerce, Science and Transportation (Oct. 24, 2017), *available at* https://www.commerce.senate.gov/public/index.cfm/pressreleases?ID=BA5E2D29-2BF3-4FC7-A79D-58B9E186412C

[437] U.S. Senate Committee on Commerce, Science and Transportation, Notice of Hearing " *Driving Automotive Innovation and Federal Policies*" on Jan. 24, 2018, *available at* https://www.commerce.senate.gov/public/index.cfm/hearings?ID=68CDF867-FFB6-425B-BD24-9542E35AC767

[438] Press Release, Federal Trade Commission (Jun. 28, 2017), *available at* https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected

[439] Federal Trade Commission, Acting Chairman's Opening Remarks, Connected Car Workshop, Jun. 28, 2017, at 5, *available at* https://www.ftc.gov/system/files/documents/public_statements/1227733/ohlhausen_-_connected_cars_workshop_opening_remarks_6-28-17.pdf

[440] Jimmy H. Koo, *Regulators, Carmakers Plot Road to Connected Car Privacy, Security* , Bloomberg News, Jun. 29, 2017, *available at* https://www.bna.com/regulators-carmakers-plot-n73014460960/

[441] *Flynn v. FCA US LLC* , No. 15-cv-00855-MJR-DGW, 2016 WL 5341749, at *1 (S.D. Ill. Sept. 23, 2016).

[442] *Id* . at *2–4.

[443] *Flynn v. FCA US LLC* , No. 15-cv-00855-MJR-DGW, 2017 WL 3592040, at *5 (S.D. Ill. Aug. 21, 2017).

[444] Plaintiffs' Motion for Class Certification at 1, *Flynn v. FCA US LLC*, No. 15-cv-00855-MJR-DGW (S.D. Ill. Oct. 13, 2017), ECF No. 266.

[445] *See* FCA US LLC's Motion for Summary Judgment and Brief in Support at 1, *Flynn v. FCA US LLC*, No. 15-cv-00855-MJR-DGW (S.D. Ill. Oct. 5, 2017), ECF No. 256.

[446] *See* Plaintiffs' Memorandum in Opposition to FCA US LLC's Motion for Summary Judgment (Filed Under Seal and Redacted in Its Entirety), *Flynn v. FCA US LLC*, No. 15-cv-008855-MJR-DGW (S.D. Ill. Nov. 6, 2017), ECF No. 278.

[447] *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955, 974 (N.D. Cal. 2015).

[448] *See Cahen v. Toyota Motor Corp.* , No. 16-15496, 2017 WL 6525501, at *1 (9th Cir. Dec. 21, 2017).

[449] *Id.*

[450] Complaint, *Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 17-CV-00039-JD (N.D. Cal. Jan. 5, 2017), ECF No. 1.

[451] *Id* . at 5–6, 8, 11–13.

[452] *Id* . at 10–13.

[453] *See Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-cv-00039-JD, 2017 WL 4150873, at *1–2 (N.D. Cal. Sept. 19, 2017).

[454] *See id.* at 6.

[455] *In re Vizio, Inc., Consumer Privacy Litig.* , No. 8:16-ml-02693 (C.D. Cal. Apr. 11, 2016).

[456] Order Denying Defendants' Motion to Dismiss and Strike, *In re: Vizio, Inc., Consumer Privacy Litigation*, 8:16-ml-02693-JLS-KES (C.D. Cal July 25, 2017), ECF No. 199; s *ee supra* pp. 2, 35-36, 41 and *infra* p. 46.

[457] *Siegel v. Samsung Electronics America, Inc. et al* ., No. 2:17-cv-01687 (D.N.J. Mar. 10. 2017), ECF. No. 1.

[458] *Id*., ECF No. 18.

[459] *In re Sling Media Slingbox* , No. 17-1094 (2d. Cir. Apr. 18, 2017).

[460] *Id.*

[461] *Rushing v. Viacom Inc.*, No. 3:17-CV-4492 (N.D. Cal. Aug. 7, 2017).

[462] *Id*., at 20-21.

[463] *Id*., at 22.

[464] Press Release, Federal Trade Commission (June 21, 2017), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business

[465] Press Release, Federal Trade Commission (Oct. 23, 2017), *available at* https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf

[466] Federal Bureau of Investigation, Consumer Notice: Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children (July 17, 2017), *available at* https://www.ic3.gov/media/2017/170717.aspx .

[467] Internet of Things: Privacy & Security in a Connected World, FTC Staff Report (January 2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf .

[468] *Federal Trade Commission, Attorney General of the State of New Jersey v. Vizio Inc. et al*, 2:17-cv-00758 (Feb. 6, 2017)

[469] The FTC asserted that Vizio violated the unfairness and deception prongs of Section 5 of the FTC Act and that Vizio's actions caused or were likely to cause "substantial injury" to consumers—a conclusion about which Acting Chair Maureen Ohlhausen expressed skepticism in a concurring statement. Concurring Statement of Acting Chairman Maureen K. Ohlhausen, In the Matter of Vizio, Inc., Matter No. 1623024 (Feb. 6, 2017) .

[470] *Federal Trade Commission, Attorney General of the State of New Jersey v. Vizio Inc. et al* , 2:17-cv-00758, at 3 (Feb. 6, 2017).

[471] Press Release: ENISA works together with European semiconductor industry on key cybersecurity areas, European Union Agency for Network and Information Security (May 22, 2017), available at https://www.enisa.europa.eu/news/enisa-news/enisa-works-together-with-european-semiconductor-industry-on-key-cybersecurity-areas.

[472] *Id.*

[473] California Legislative Information, SB-327 Information Privacy: connected devices, *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 .

[474] Text of proposed bill available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 .

[475] Najiyya Budaly, *Data Rules to Bring Cyber Insurance Surge, Report Says*, Law360 (Dec. 13, 2017), https://www.law360.com/articles/994267/data-rules-to-bring-cyber-insurance-surge-report-says.

[476] *Id.*; William Shaw, *Insurers Urge Leniency On Profiling Under EU Data Laws*, Law360 (Dec. 5, 2017), https://www.law360.com/cybersecurity-privacy/articles/991522/insurers-urge-leniency-on-profiling-under-eu-data-laws.

[477] Evan Weinberger, *Banks, Insurers Get More Time for NY Cybersecurity Rule*, Law360 (Dec. 21, 2016), https://www.law360.com/articles/875764/banks-insurers-get-more-time-for-ny-cybersecurity-rule.

[478] *Cybersecurity Legislation 2017*, National Conference of State Legislatures (Oct. 30, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx.

[479] Jeff Sistrunk, *A Guide to Insurance Coverage for Biometric Privacy Suits*, Law360 (Nov. 6, 2017), https://www.law360.com/cybersecurity-privacy/articles/981980/a-guide-to-insurance-coverage-for-biometric-privacy-suits.

[480] *See* Jeff Sistrunk, *Small Cos. Slow To Pick Up Cyberinsurance, Lawmakers Hear*, Law360 (July 26, 2017), https://www.law360.com/articles/947964/small-cos-slow-to-pick-up-cyberinsurance-lawmakers-hear.

[481] Budaly, *supra* note 477.

[482] *Taylor & Lieberman v. Fed. Ins. Co.*, 681 F. App'x 627, 629 (9th Cir. 2017).

[483] *Id.*

[484] *American Tooling Ctr., Inc. v. Travelers Cas. and Sur. Co. of Am.* , No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017); Jeff Sistrunk, *Travelers Tells 6th Circ. To Uphold Email Scam Coverage Win* , Law360 (Dec. 13, 2017), https://www.law360.com/articles/994258/travelers-tells-6th-circ-to-uphold-email-scam-coverage-win.

[485] *American Tooling Ctr.*, 2017 WL 3263356 at *1.

[486] Sistrunk, *supra* note 486.

[487] *American Tooling Ctr., Inc.*, 2017 WL 3263356 at *3.

[488] *Id.*

[489] *Id.*

[490] Sistrunk, *supra* note 486.

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

[492] *Id.* at * 1–2.

[493] *Id.* at *4.

[494] *Id.* at *4.

[495] *Id.* at *6.

[496] *Id.* at *7.

[497] *Id.* at *6.

[498] *Id.* at *5; *Universal American Corp. v. National Union Fire Insurance Co* ., 37 N.E.3d 78 (N.Y. 2015).

[499] Jeff Sistrunk, *Email Scam Not a Covered Fraud, Insurer Org. Tells 2nd Circ.* , Law360 (Nov. 29, 2017), https://www.law360.com/articles/989344/email-scam-not-a-covered-fraud-insurer-org-tells-2nd-circ-; *See also Posco Daewoo Am. Corp. v. Allinex USA, Inc.*, No. 17-483, 2017 WL 4922014, at *5–6 (D. N.J. Oct. 31, 2017) (granting defendant's motion to dismiss on the grounds that an email spoofing scheme and plaintiff's voluntary wire transfer did not meet the definition of computer fraud).

[500] *InComm Holdings, Inc. v. Great Am. Ins. Co*., 1:15-cv-2671-WSD, 2017 WL 1021749, at * 1–2 (N.D. Ga. Mar. 16, 2017).

[501] *Id.* at *6–7.

[502] *Id.* at *8–9.

[503] *Id.* at *11.

[504] *Spec's Family Partners, Ltd. v. The Hanover Ins. Co.*, No. H-16-438, 2017 WL 3278060, at *1 (S.D. Tex. Mar. 15, 2017).

[505] *Id.*

[506] *Id.*

[507] *Id.* at * 4–9.

[508] *Id.* at *3.

[509] *Id.* (internal quotation marks omitted).

[510] *Id.*

[511] *Id.*

[512] *Id.*at *4.

[513] *Id.* at *5.

[514] *Id.* at *8.

[515] Dave Simpson, *Children's Hospital Sues Insurer for Data Breach Coverage*, Law360 (Nov. 20, 2017), https://www.law360.com/cybersecurity-privacy/articles/987237/children-s-hospital-sues-insurer-for-data-breach-coverage.

[516] *Id.*

[517] *Id.*

[518] *Innovak Int'l, Inc. v. Hanover Ins. Co.*, No. 8:16-cv-2453-MSS-JSS, 2017 WL 5632718, at * 6–7 (M.D Fla. Nov. 17, 2017); Jeff Sistrunk, *Insurer Doesn't Owe Defense of Data Breach Suit, Judge Says* , Law360 (Nov. 17, 2017), https://www.law360.com/cybersecurity-privacy/articles/986792/insurer-doesn-t-owe-defense-of-data-breach-suit-judge-says.

[519] *Report: TCPA Consumer Litigation Filings on Track to End 2017 Under Recent Annual Totals* , ACA International (Nov. 28, 2017), https://www.acainternational.org/news/report-tcpa-consumer-litigation-filings-on-track-to-end-2017-under-recent-annual-totals.

[520] *Spokeo, Inc. v. Robins* , 136 S. Ct. 1540, 1545, 1549–50 (2016).

[521] 15 U.S.C. § 1681 *et seq.*

[522] 15 U.S.C. §§ 1681(n), 1681(o).

[523] Judgement, *Sergio L. Ramirez v. Trans Union, LLC*, No. 12-cv-00632-JSC (June 21, 2017) ECF No. 309; *see also* Order Re: Plaintiff Sergio Ramirez's Motion for a Service Award, *Sergio L. Ramirez v. Trans Union, LLC*, No. 12-cv-00632-JSC (Nov. 7, 2017) ECF No. 345.

[524] *Id.*

[525] *Sergio Ramirez v. Trans Union LLC* , No. 17-17244 (9th Cir. docketed Nov. 02, 2017).

[526] *See* 15 U.S.C. § 1681e(b).

[527] *Pedro v. Equifax, Inc.* , 868 F.3d 1275, 1281 (11th Cir. 2017) (internal quotation marks omitted) (finding credit reporting agency's interpretation of the FCPA was not objectively unreasonable given judicial precedent, though expressing preference for a more exacting interpretation).

[528] *Id.* at 1283 (Rosenbaum, R., concurring) (internal quotation marks omitted) (citing *Alexander v. Moore & Assocs., Inc.*, 553 F. Supp. 948, 952 (D. Haw. 1982)).

[529] *See* 15 U.S.C. § 1681b(b)(2)(A).

[530] *Hargrett v. Amazon.com DEDC LLC* , 235 F. Supp. 3d 1320 (M.D. Fla. 2017) (denying defendant's motion to dismiss for lack of Article III standing for FCRA claims).

[531] *Anderson v. Wells Fargo Bank, N.A.* , 266 F. Supp. 3d 1175 (D.S.D. 2017) (holding plaintiffs' claims were time-barred though they would have had Article III standing to pursue FCRA claims).

[532] *In re Michaels Stores, Inc., Fair Credit Reporting Act (FCRA) Litig.* , No. 2615, 2017 WL 354023 (D.N.J. Jan. 24, 2017) (dismissed for lack of Article III standing).

[533] *Saltzberg vs. Home Depot U.S.A., Inc.* , No. 2:17-CV-05798, 2017 WL 4776969 (C.D. Cal. Oct. 18, 2017) (dismissed for lack of Article III standing).

[534] *See* Compl., *Microsoft Corp. v. U.S. Dep't of Justice ("Microsoft")*, No. 2:16-cv-00538-JLR (W.D. Wash. Apr. 14, 2016), ECF No. 1.

[535] 18 U.S.C. § 2705(b). Specifically, a court must grant a government application for a nondisclosure order if it finds reason to believe that disclosure will result in: (1) Endangering the life or physical safety of an individual; (2) Flight from prosecution; (3) Destruction or tampering with evidence; (4) Intimidation of potential witnesses; or (5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial. *Id.*

[536] *See* First Am. Compl., ¶ 5, *Microsoft*, No. 2:16-cv-00538-JLR (W.D. Wash. June 17, 2016), ECF No. 28.

[537] Unopposed Motion for Leave to File Brief of Amici Curiae, *Microsoft*, No. 2:16-cv-00538-JLR (W.D. Wash. June 17, 2016), ECF No. 49.

[538] Motion for Leave to File Brief of Amici Curiae, *Microsoft*, No. 2:16-cv-00538-JLR (W.D. Wash. June 17, 2016), ECF No. 58.

[539] Stipulated Motion for Leave to File Brief of Amici Curiae, *Microsoft*, No. 2:16-cv-00538-JLR (W.D. Wash. June 17, 2016), ECF No. 56.

[540] Unopposed Motion for Leave to File Brief as Amici Curiae, *Microsoft*, No. 2:16-cv-00538-JLR (W.D. Wash. June 17, 2016), ECF No. 66.

[541] *See Microsoft Corp. v. U.S. Dep't of Justice* , 233 F. Supp. 3d 887, 889–902 (W.D. Wash. 2017).

[542] *Id* . at 907–08.

[543] *Id.* at 915–16.

[544] U.S. Dep't of Justice, Memorandum re Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b) (Oct. 19, 2017), *available at* https://www.justice.gov/criminal-ccips/page/file/1005791/download.

[545] *Id.* at 2. The policy memo cites "national security investigations that materially differ from routine criminal investigations" as an example of what might constitute "exceptional circumstances." *Id.* at 2 n.3.

[546] *See* Microsoft Corporation's Unopposed Motion for Voluntary Dismissal at 2, *Microsoft*, No. 2:16-cv-00538-JLR (W.D. Wash. Oct. 24, 2017), ECF No. 117; *see also* Order Granting Microsoft Corporation's Unopposed Motion for Voluntary Dismissal (W.D. Wash. Oct. 25, 2017), ECF No. 119.

[547] *United States v. Carpenter* , 819 F.3d 880, 884–85 (6th Cir. 2016).

[548] *Id.* at 884–86.

[549] *Id.* at 885.

[550] *Id.* at 884.

[551] *Id.* at 887.

[552] *Smith v. Maryland* , 442 U.S. 735, 740 (1979).

[553] *United States v. Miller* , 425 U.S. 435, 440 (1976).

[554] Brief for United States at 15–18, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 4311113.

[555] *Id.* at 43–52.

[556] Brief for Petitioner at 15, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 3575179; see also *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment) "[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

[557] *Id.* at 26–29.

[558] Brief of the Center for Democracy and Technology as Amicus Curiae, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 3530958.

[559] Brief for the Competitive Enterprise Institute, et al. as Amici Curiae, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 3530955.

[560] Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Thirty-Six Technical Experts, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 3530960.

[561] Brief Amici Curiae for The Reporters Committee for Freedom of the Press and 19 Media Organizations, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 3530966.

[562] Brief for Scholars of Criminal Procedure and Privacy as Amici Curiae, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 3614233.

[563] Brief for Technology Experts as Amici Curiae, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 3530967.

[564] Amicus Curiae Brief for National District Attorneys Association, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 4417212.

[565] Brief for the States of Alabama, et al. as Amici Curiae, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 4417211.

[566] Brief of Professor Orin S. Kerr as Amicus Curiae, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 4417210.

[567] Brief for Technology Companies as Amici Curiae, *Carpenter v. United States*, __ U.S. __ (2018) (No. 16-402), 2017 WL 3601390.

[568] S. 1654, 115th Cong. (2017).

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

[570] S. 1654, 115th Cong. § 3 (2017).

[571] S. 1657, 115th Cong. (2017).

[572] S. 1657, 115th Cong. § 2 (2017).

[573] S. 1657, 115th Cong. § 4 (2017).

[574] U.S. Dep't of Justice, Memorandum re Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b) (Oct. 19, 2017), *available at* https://www.justice.gov/criminal-ccips/page/file/1005791/download.

[575] The ECPA Modernization Act of 2017 defines "geolocation information" to mean "any information concerning the past or current location of an electronic communications device that is in whole or in part generated by or derived from the operation or use of the electronic communications device," and defines "geolocation service" to mean "the provision of a service or functionality that uses or collects geolocation information." S. 1657, 115th Cong. § 5 (2017).

[576] S. 1657, 115th Cong. § 2 (2017).

[577] 18 U.S.C. § 2703(d).

[578] *Id* .

[579] S. 1657, 115th Cong. § 5 (2017).

[580] Sophia Cope, *EFF Supports Senate Email and Location Privacy Bill*, Eff.org (Jul. 27, 2017), https://www.eff.org/deeplinks/2017/07/eff-applauds-senate-email-and-location-privacy-bill (last visited Dec. 20, 2017).

[581] American Civil Liberties Union, *ACLU Statement On Introduction Of Electronic Communications Privacy Modernization Act* , aclu.org (Jul. 27, 2017), https://www.aclu.org/news/aclu-statement-introduction-electronic-communications-privacy-modernization-act (last visited Dec. 20, 2017).

[582] Adam Brandon, *Support the ECPA Modernization Act, S. 1657*, Freedomworks.org (Jul. 31, 2017), http://www.freedomworks.org/content/support-ecpa-modernization-act-s-1657 (last visited Dec. 20, 2017).

[583] Deborah Collier, *ECPA Modernization Act of 2017 Introduced* , cagw.org (Jul. 27, 2017), https://www.cagw.org/thewastewatcher/ecpa-modernization-act-2017-introduced (last visited Dec. 20, 2017).

[584] Consumer Technology Association, *CTA Applauds Senate for Bipartisan ECPA Reform Bill*, cta.tech (Jul. 27, 2017), https://www.cta.tech/News/Press-Releases/2017/July/CTA-Applauds-Senate-for-Bipartisan-ECPA-Reform-Bil.aspx (last visited Dec. 20, 2017).

[585] Chris Calabrese, *The Bill Our Privacy Desperately Needs in the Digital Age*, Cdt.org (Jul. 27, 2017), https://cdt.org/blog/the-bill-our-privacy-desperately-needs-in-the-digital-age/ (last visited Dec. 20, 2017).

[586] Ivan Dominguez, Ezra Dunkle-Polier, Alexandra Funk, *NACDL News: NACDL Welcomes Introduction of Bipartisan ECPA Modernization Act of 2017* (Aug. 2017), nacdl.org, https://www.nacdl.org/Champion.aspx?id=48305 (last visited Dec. 20, 2017).

[587] Brad Smith, *DOJ acts to curb the overuse of secrecy orders. Now it's Congress' turn* , Microsoft.com (Oct. 23, 2017), https://blogs.microsoft.com/on-the-issues/2017/10/23/doj-acts-curb-overuse-secrecy-orders-now-congress-turn/ (last visited Dec. 20, 2017).

[588] *Compare In re Grand Jury Subpoena Duces Tecum Dated Mar. 25 , 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (holding that providing a password is a testimonial act), *and* Order Denying Application to Compel Decryption, *In re The Decryption of a Seized Data Storage System*, Case No. 13-M-449 (E.D. Wisc. Apr. 19, 2013) (same), *with United States v. Fricosu*, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (holding production of unencrypted drive by defendant did not implicate Fifth Amendment right against self-incrimination), *and Commonwealth v. Gelfgatt*, SUCR2010-10491 (Sup. Ct. Mass. Nov. 6, 2014) (holding defendant in contempt for failure to unlock password protected drives), and *State v. Stahl*, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016) (quashing order denying motion to compel production of cell

phone passcode and noting that "we are not inclined to believe that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals who use their fingerprint as the passcode").

[589] *See, e.g.* , *Com. v. Baust*, 89 Va. Cir. 267 (Va. Cir. Ct. 2014) (granting motion to compel defendant to unlock phone with fingerprint and noting that "like physical characteristics that are non-testimonial, the fingerprint of Defendant if used to access his phone is likewise non-testimonial and does not require Defendant to 'communicate any knowledge' at all."); *State v. Diamond*, 890 N.W.2d 143, 150 (Minn. Ct. App. 2017), review granted (Mar. 28, 2017) ("By being ordered to produce his fingerprint, [defendant] was not required to disclose any knowledge he might have or to speak his guilt."); *but see* Opinion and Order at 11-14, *In re Application for a Search Warrant*, No. 1:17-mc-00081 (N. D. Il. Feb. 16, 2017), ECF No. 1 (denying application for warrant to compel all individuals present during execution to use fingerprints to unlock "any Apple iPhone, iPad, or other Apple brand device" and noting that "[t]he connection between the fingerprint and Apple's biometric security system, shows a connection with the suspected contraband.")

[590] *See* Oleg Afonin, *New Security Measures in iOS 11 and Their Forensic Implications* , Elcomsoft.com (Sep. 7, 2017), https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/ (last visited Dec. 20, 2017).

[591] *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014), *rev'd*, 829 F.3d 197 (2d Cir. 2016).

[592] Brief for Microsoft at 17-18, *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.* , 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014), *rev'd*, 829 F.3d 197 (2d Cir. 2016).

[593] *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d at 467, *rev'd*, 829 F.3d 197 (2d Cir. 2016).

[594] *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.* , 829 F.3d 197, 201 (2d Cir. 2016), *cert. granted, United States v. Microsoft Corp.*, No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017).

[595] *Id.* at 214-20.

[596] *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.* , 855 F.3d 53, 76 (2d Cir. 2017) (Carney, J., concurring) (denying rehearing en banc).

[597] *Id.* at 55-56 (Carney, J., concurring).

[598] *Id.* at 61 (Jacobs, J., dissenting); *Id.* at 63, 66 (Cabranes, J., dissenting); *Id.* at 70 (Raggi, J., dissenting); *Id.* at 75 (Droney, J., dissenting).

[599] *Id.* at 61 (Jacobs, J., dissenting).

[600] *Id.* at 63, 66 (Cabranes, J., dissenting).

[601] *Id.* at 75 (Droney, J., dissenting).

[602] *In re Search of Info. Associated with [redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.* , No. 16-MJ-00757 (BAH), 2017 WL 3445634 (D.D.C. July 31, 2017); *Matter of Search of Content Stored at Premises Controlled by Google Inc.* , No. 16-MC-80263-RS, 2017 WL 3478809 (N.D. Cal. Aug. 14, 2017); *In re Search Warrant No. 16-960-M-1 to Google*, No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017).

[603] *In re Search of Info. Associated with [redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.* , 2017 WL 3445634, at *16, *23-24; *Matter of Search of Content Stored at Premises Controlled by Google Inc.* , 2017 WL 3478809, at *3; *In re Search Warrant No. 16-960-M-1 to Google*, 2017 WL 3535037, at *7-9.

[604] *United States v. Microsoft Corp.* , No. 17-2, 2017 WL 2869958, at *1 (U.S. Oct. 16, 2017).

[605] Brief for Petitioner at 21-25, *United States v. Microsoft Corp.*, No. 17-2, 2017 WL 2869958 (U.S. Dec. 6, 2017).

[606] *Id.* at 29-31.

[607] *Id.* at 26-28.

[608] *Id.* at 32-37.

[609] *Id.* at 42-43.

[610] Brief for Respondent at 20-37, *United States v. Microsoft Corp.*, No. 17-2, 2017 WL 2869958 (U.S. Jan. 11, 2018).

[611] *Id.* at 19.

[612] Comput. Crime & Intellectual Prop. Section, Criminal Div., U.S. Dep't of Justice, Seeking Enterprise Customer Data Held by Cloud Service Providers, at 1 (Dec. 2017), https://www.justice.gov/criminal-ccips/file/1017511/download.

[613] *Id.* at 2.

[614] *Id.* at 2-3.

[615] Neal Suggs, *DOJ's Newly Released Recommended Practices Are a Win for Cloud and Enterprise Customers* , Microsoft (Dec. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/12/14/new-doj-guidelines-win-cloud-enterprise-customers.

[616] 50 U.S.C. §§ 1801-1885.

[617] 50 U.S.C. § 1802(a)(1).

[618] 50 U.S.C. § 1801(e).

[619] *See* http://www.fisc.uscourts.gov/ (*last visited* Dec. 20, 2017).

[620] Barton Gellman and Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program* , The Washington Post, *available at* https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

[621] *See Decoding 702: What is Section 702* , Elec. Frontier Found., https://www.eff.org/702-spying.

[622] *See Reauthorizing FISA Section 702*, The Heritage Found., http://www.heritage.org/reauthorizing-fisa-section-702 .

[623] *See Decoding 702: What is Section 702* , Elec. Frontier Found., https://www.eff.org/702-spying.

[624] Dustin Volz, *Trump signs bill renewing NSA's internet surveillance program* , Reuters (Jan. 19, 2018), https://www.reuters.com/article/us-usa-trump-cyber-surveillance/trump-signs-bill-renewing-nsas-internet-surveillance-program-idUSKBN1F82MK.

[625] FISA Amendments Reauthorization Act of 2017, S. 2010, 115th Congr., *available at* https://www.congress.gov/bill/115th-congress/senate-bill/2010 ; *see also* Daniel Wilson, *Senate Intel Panel Approves Renewal of Surveillance Powers*, Law 360, https://www.law360.com/articles/978227/senate-intel-panel-approves-renewal-of-surveillance-powers .

[626] *See id.*

[627] Daniel Wilson, *House Panel Approves Surveillance Renewal Bill*, Law 360, https://www.law360.com/articles/989972/house-panel-approves-surveillance-renewal-bill .

[628] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, *available at* http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

[629] Art. 3, ¶ 2, GDPR.

[630] Art. 3, ¶ 2(b), GDPR.

[631] Art. 7, GDPR.

[632] *Id.*

[633] Art. 35, GDPR.

[634] *Id.*

[635] *Id* .

[636] Art. 44–48, GDPR.

[637] Art. 83, ¶¶ 4–5, GDPR.

[638] European Commission, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield* 2 (2017), *available at* http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619.

[639] *Id.* at 4.

[640] *Id.* at 4–7.

[641] Press Release, Federal Trade Commission, FTC Gives Final Approval to Settlements with Companies that Falsely Claimed Participation in Privacy Shield (Nov. 29, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/11/ftc-gives-final-approval-settlements-companies-falsely-claimed .

[642] *See* FT Cyber Security, "China's cyber security law rattles multinationals," *Financial Times* (May 30, 2017), *available at* https://www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996 .

[643] Alex Lawson, "US Asks China Not To Implement Cybersecurity Law," Law360 (Sept. 27, 2017) *available at* https://www.law360.com/articles/968132/us-asks-china-not-to-implement-cybersecurity-law.

[644] Sophie Yan, "China's new cybersecurity law takes effect today, and many are confused," CNBC.com (June 1, 2017), *available at* https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html.

[645] Christina Larson, Keith Zhai, and Lulu Yilun Chen, "Foreign Firms Fret as China Implements New Cybersecurity Law", Bloomberg News (May 24, 2017), *available at* https://www.bloomberg.com/news/articles/2017-05-24/foreign-firms-fret-as-china-implements-new-cybersecurity-law .

[646] Clarice Yue, Michelle Chan, Sven-Michael Werner and John Shi, "China Cybersecurity Law update: Draft Guidelines on Security Assessment for Data Export Revised!," Lexology (Sept. 26, 2017), *available at* https://www.lexology.com/library/detail.aspx?g=94d24110-4487-4b28-bfa5-4fa98d78a105 .

[647] Singapore Personal Data Protection Commission, Proposed Advisory Guidelines on the Personal Data Protection Act For NRIC Numbers, published 7 November 2017, *available at* https://www.pdpc.gov.sg/docs/default-source/public-consultation-6---nric/proposed-nric-advisory-guidelines---071117.pdf?sfvrsn=4 .

[648] Office of the Australian Information Commissioner, "De-identification Decision-Making Framework", Australian Government (Sept. 18, 2017), *available at* https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-decision-making-framework ; Lyn Nicholson, "Regulator issues new guidance on de-identification and implications for big data usage", *Lexology* (Sept. 26, 2017) *available at* https://www.lexology.com/library/detail.aspx?g=f6c055f4-cc82-462a-9b25-ec7edc947354; "New Regulation on the Deletion, Destruction or Anonymization of Personal Data," British Chamber of Commerce of Turkey (Sept. 28, 2017), *available at* https://www.bcct.org.tr/news/new-regulation-deletion-destruction-anonymization-personal-data-2/64027 ; Jena M. Valdetero and David Chen, "Big Changes May Be Coming to Argentina's Data Protection Laws," Lexology (June 5, 2017), *available at* https://www.lexology.com/library/detail.aspx?g=6a4799ec-2f55-4d51-96bd-3d6d8c04abd2.

[649] Naïm Alexandre Antaki and Wendy J. Wagner, "No escaping notification: Government releases proposed regulations for federal data breach reporting & notification", *Lexology* (Sept. 6, 2017), *available at* https://www.lexology.com/library/detail.aspx?g=0a98fd33-1f2c-4a52-98c0-cf1feeaf0b90 ; Ministry of Electronics & Information Technology, "White Paper of the Committee of Experts on a Data Protection Framework for India," Government of India (Nov. 27, 2017), *available at* http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited .

The following Gibson Dunn lawyers assisted in the preparation of this client alert: Alexander Southwell, Joshua Jessen, Caroline Krass, Eric Vandevelde, Ryan Bergsieker, Abbey Barrera, Kamola Kobildjanova, Lindsey Young, Amy Chmielewski, Melissa Goldstein, Alex Murchison, Reid Rector and Ilissa Samplin, with contributions from Angelica Agishi, Jacob Arber, Stephanie Balitzer, Melinda Biancuzzo, Sheli Chabon, Alli Chapin, Soolean Choy, Josiah Clarke, Tim Deal, Amanda George, Zoey Goldnick, Christian Hudson, Jordan Jacobsen, Miranda Lievsay, Ian Long, Cary McClelland, Jon Newmark, Sheri Pan, Nathan Powell, Jacob Rierson, Alon Sachar, Nick Scheiner, Sydney Sherman, Frances Smithson, Sam Spears, Marc Takagaki, Kayla Wieche and Alex Zbrozek.

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 group:

United States

Alexander H. Southwell - Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)

Caroline Krass - Chair, National Security Practice, Washington, D.C. (+1 202-887-3784, ckrass@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)

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)
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)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)

Europe
Ahmed Baladi - 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)
Bernard Grinspan - Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Jean-Philippe Robé - Paris (+33 (0)1 56 43 13 00, jrobe@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Nicolas Autet - Paris (+33 (0)1 56 43 13 00, nautet@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Emmanuelle Bartoli - Paris (+33 (0)1 56 43 13 57, ebartoli@gibsondunn.com)
Alejandro Guerrero Perez - Brussels (+32 2 554 7218, aguerreroperez@gibsondunn.com)

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

Questions about SEC disclosure issues concerning data privacy and cybersecurity can also be addressed to the following leaders and members of the Securities Regulation and Corporate Disclosure Group:

James J. Moloney - Orange County, CA (+1 949-451-4343, jmoloney@gibsondunn.com)
Elizabeth Ising - Washington, D.C. (+1 202-955-8287, eising@gibsondunn.com)
Lori Zyskowski - New York (+1 212-351-2309, lzyskowski@gibsondunn.com)