GIBSON DUNN

U.S. Cybersecurity and Data Privacy Outlook and Review – 2020

Client Alert | January 27, 2020

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

In 2019, companies, courts, and regulators faced unprecedented challenges as they navigated a rapidly evolving set of cybersecurity and privacy issues. Congress and state legislatures proposed (and, in the case of some states, enacted) measures ranging from limits on the use of consumer data to protecting children's internet privacy. Increasingly active federal and state regulators enforced data privacy, cybersecurity, and consumer protection standards in the face of novel cybersecurity threats. Private parties stepped up the pace of civil litigation in a year that saw numerous high-profile data breaches and continued questions over who can sue for damages. And questions regarding the government's ability to access data, from biometric information to files stored overseas, came into sharper legislative and judicial focus.

This Review places these, and other, 2019 developments in broader context, addressing: (1) the regulation of privacy and data security, including key legislative developments, enforcement actions by federal and state authorities, and new regulatory guidance; (2) trends in civil litigation around data privacy issues in areas including privacy class actions, digital communications, and biometric information privacy laws; and (3) the collection of electronically stored information by government actors, including the extraterritoriality of subpoenas and warrants and the collection of data from electronic devices. While we do not attempt to address every development that occurred in 2019, this Review examines a number of the most significant developments affecting companies as they navigate the evolving cybersecurity and privacy landscape.

This Review focuses on cybersecurity and privacy developments within the United States. For information on developments outside the United States, please see Gibson Dunn's International Cybersecurity and Data Privacy Outlook and Review, which addresses developments in 2019 outside the United States that are of relevance to domestic and international companies alike. We have adopted the practice of referring to companies by generic descriptors in the body of the alert; for further details, please see the endnotes.

Related People

Ryan T. Bergsieker

Timothy W. Loose

Ashley Rogers

Chris Connelly

Sarah E. Erickson

Cassandra L. Gaedt-Sheckter

Nicole Lee

Isabella R. Sayyah

Jeremy S. Smith

Table of Contents

I. Regulation of Privacy and Data Security

A. Legislative Developments

1. State

a) California Consumer Privacy Act of 2018

As the first comprehensive consumer privacy law in the United States, the California Consumer Privacy Act of 2018 ("CCPA") has changed the legal landscape. According to one observer, initial compliance with the CCPA will cost businesses around $55 billion.[1] As reported in detail in Gibson Dunn's prior CCPA updates,[2] the law requires businesses to disclose what personal information they collect from California consumers (defined broadly as California residents), for what purpose, and to what third parties the information is shared or sold. The law also allows consumers the right to request deletion of their personal information and opt out of the sale of such information, among other provisions.

Despite passing in 2018, and coming into effect in January 2020, the law continued to

evolve in 2019, and is still evolving. California's Attorney General is set to release final regulations in the first part of 2020 (at the time of publishing this Review only a draft version of the regulations had been released, in October 2019).[3] Further, the California legislature passed multiple amendments just two months before the law became effective,[4] and continued attempts at amending the law are expected, along with another ballot initiative in November 2020 that would expand the CCPA's reach.[5] And despite clarifying amendments and draft regulations aimed at implementing the CCPA, there are still a number of open issues for businesses to analyze.

As an example, the scope of "sale" continues to be the subject of extensive debate. The CCPA regulates the "sale" of personal information, which it defines as the exchange of personal information "for monetary or other valuable consideration."[6] This definition creates some uncertainty for businesses that do not expressly sell user data in a traditional sense, but may receive some tangible benefit from sharing the data with a third party. In addition, where data is automatically collected and analyzed by a third party using web-browser cookies, it can be technologically difficult or impossible to identify what information is associated with the particular consumer and to wholly comply with the consumer's request. Separately, the law's private right of action for subjects of certain data breaches caused by a lack of "reasonable" security protections has caused concern regarding what constitutes "reasonable," particularly in light of the statute's potentially steep statutory damages.[7]

While California's Attorney General will not bring enforcement actions under the CCPA until July 1, 2020, the law went into effect January 1, 2020, and the Attorney General indicated in late 2019 that he may consider prosecuting businesses not in compliance with the law as of the effective date.[8] That said, the Attorney General also has reported that enforcement initially will focus on companies that deal in large amounts of sensitive personal data—such as health data and Social Security numbers[9]—and on companies that collect the personal data of children.[10] Meanwhile, the CCPA's narrow private right of action for data breaches is already in full effect.[11] While as of the time of this writing no such actions have been widely reported as filed, Gibson Dunn will continue to monitor CCPA-related developments.

b) Other State Laws

Aside from the CCPA, several other states also considered, passed, or began enforcement on their own data privacy and consumer protection laws in 2019.

i. Nevada

On October 1, 2019 Nevada's "Act relating to Internet privacy" went into effect.[12] Compared to the CCPA, Nevada's privacy law has a narrower definition of "sale" of personal information: "the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons."[13] This definition does not include the CCPA's broader definition of an exchange of covered information for "other valuable consideration." The Nevada law also has a narrower definition of "consumer"—a "consumer" is a "person who seeks or acquires, by purchase or lease, any good, service, money or credit for personal, family or household purposes from the Internet website or online service of an operator." The law excludes from the definition of "operator": (1) financial institutions and affiliates subject to the GLBA; (2) HIPAA-covered entities; and (3) certain manufacturers of motor vehicles and persons who repair or service motor vehicles.[14]

The law requires that website operators provide an online notice disclosing what covered information the operators maintain, and requires that they permit consumers to opt out of any sale of such information by the website to third parties.[15] Nevada's privacy law contains no private right of action, and caps penalties at $5,000 per violation.[16]

ii. Maine

Like Nevada, Maine's new data privacy law, "An Act to Protect the Privacy of Online Customer Information," which will go into effect July 1, 2020, is narrower than the CCPA in many ways.[17] For example, it applies only to broadband providers in Maine and affects only those who are physically located and billed for broadband services in Maine.[18] The Act generally prohibits broadband providers from using, disclosing, selling, or permitting nonconsensual access to their customers' personal information. The law imposes a transparency requirement on broadband providers to publish privacy notices informing customers of their rights and of the provider's obligations at the point of sale. Similar to the CCPA, the law prohibits broadband providers from refusing service to customers who do not provide their consent or charging customers a penalty or offering customers a discount based on the customer's decision to provide consent or not.[19]

iii. New York

The Stop Hacks and Improve Electronic Data Security ("SHIELD") Act modifies New York's data breach law by changing the definition of a data breach to include any unauthorized person gaining access to or acquisition of the protected information.[20] The Act also expands upon the definition of "private information" to include, in conjunction with a New York resident's name, number, personal mark or other identifier, the following data: (1) bank account, credit, or debit card number, provided that the numbers could be used to access an individual's account without more; and (2) biometric information.[21] The Act also adds to the definition of "private information" usernames or email addresses accompanied with passwords or security questions and answers that would grant access to an online account.[22] The Act requires covered entities to establish data security programs to safeguard personal user data, safeguards that are tailored to the size of the business.[23] The Act relieves covered entities, however, of their notification obligations if a breach was the result of an inadvertent disclosure by persons authorized to access private information and the entity determines that the exposure is unlikely to result in harm to the affected individuals. However, if the breach affects over 500 New York residents, the covered entity must provide a written determination as to the risk of harm to these individuals to the New York Attorney General.[24] Notably, 2019 also saw legislative attempts, ultimately unsuccessful, for New York to pass the New York Privacy Act,[25] a proposed law offering protections as broad, or broader, than those provided by the CCPA, as discussed more fully below.[26]

c) State Laws Under Consideration

Numerous states considered privacy legislation in 2019, and many of those states are expected to revive their failed 2019 bills in 2020.[27] For example, Washington is expected to adopt a version of the "Washington Privacy Act"—previously stalled in 2019—which, in addition to adopting many of the CCPA's provisions, would set limits on the commercial use of facial recognition technology and would grant consumers the right to confirm whether a controller is processing personal data about the consumer and to access that data, to correct inaccurate data, to delete personal data, and to clearly opt out of the use of personal information for targeted advertising.[28] The draft legislation provides for no private right of action and caps penalties at $7,500 per violation.[29]

In addition, New York, Florida, Texas, Massachusetts, New Jersey, Virginia, and New Hampshire are a few of the many states considering adopting comprehensive privacy laws similar to CCPA (in the absence of preemptive federal legislation). In particular, New York's proposed law contains more stringent requirements than the CCPA.[30] It would require consumer opt-in before a company could use, process, sell, share, or transfer that consumer's data, and would impose upon controllers and data brokers who collect, sell, or license personal data a fiduciary duty of care, loyalty, and confidentiality.[31] The New York proposed law would also allow for a private right of action.[32] With so many

diverging state privacy bills passed or gaining traction, many businesses are rightfully concerned that 2020 signals the beginning of a patchwork of comprehensive state privacy laws, resulting in an even more complex compliance environment.[33]

2. Federal

a) Comprehensive Privacy Legislation

Three comprehensive privacy bills are currently being considered in Congress, each discussed below. Democrats have published a "Senate Democratic Privacy Principles" list of minimum provisions required in any Democratic-backed privacy legislation,[34] and favor a federal privacy law that includes a private right of action.[35] Republicans favor a law that explicitly preempts state privacy laws like those in California, Nevada, and Maine.[36] Many commentators have suggested that enacting federal privacy legislation will be difficult in 2020 given the federal elections, and expect states to be more successful in enacting privacy legislation.[37] Indeed, comprehensive federal privacy legislation has been a topic of discussion for many years, but such legislation has not yet been enacted.

i. House Energy and Commerce Committee Staff Bipartisan Draft Privacy Bill

One bill that is likely to see action in 2020 is a bipartisan staff draft out of the House Energy and Commerce Committee. The House Energy and Commerce Committee draft bill is more comprehensive than the CCPA because it establishes within the FTC a specialized enforcement arm, the Bureau of Privacy, and an Office of Business Mentorship to assist with compliance.[38] Many parts of the bill, however, are still in flux.[39] Notably, it does not, in its current form, contain a private right of action or address state law preemption, despite advocates both proposing and opposing such measures.[40] In terms of consumers, the proposal would include, among other protections the right to request to know information collected and the purpose of collection; the right to correct personal information; the right to request to delete information; and the ability to port that information to another service provider.[41]

The draft bill also places requirements on businesses, similar to those of the European Union's GDPR: maintaining privacy policies; implementing a privacy program and establishing reasonable policies, practices and procedures for the processing of covered data; designating a privacy protection officer; and seeking affirmative consent for the processing of covered data unless the processing is "consistent with the reasonable consumer expectations within the context of the interaction between the covered entity and the individual."[42] Additionally, large companies would be required to provide annual filings to the FTC, including the results of an internal risk assessment and measures taken to address those risks. The bill also mandates express affirmative consent for all processing of sensitive information, which consent must be given separately for each type of personal information processed.[43]

While the draft bill is a step toward a bipartisan, comprehensive privacy law, at the time of publishing this Review, the two major political parties have not reached an agreement regarding several sections of the bill, including exceptions to the consent requirement, categorization of sensitive data and de-identified data, revenues and amounts of data processing sufficient to require heightened compliance from companies; opt-out requirements for first-party marketing; discriminatory use of data; and the size of the Bureau of Privacy; along with the issues of preemption and a private right of action.[44]

ii. Consumer Online Privacy Rights Act and United States Consumer Data Privacy Act of 2019

The proposed Consumer Online Privacy Rights Act ("COPRA"),[45] introduced by Senator

Maria Cantwell (D-WA), and the draft United States Consumer Data Privacy Act of 2019 ("CDPA"),[46] circulated by Senator Roger Wicker (R-MS), Chairman of the Senate Commerce Committee, share many of the features included in the House Energy and Commerce Committee staff bipartisan draft privacy bill, requiring companies to adopt privacy policies and risk-based data security practices and assessments, and provide consumers the right to access, correct, delete, and port their data.[47] The Democrat-backed COPRA contains a private right of action while CDPA does not, and CDPA contains broad state-law preemption, while COPRA generally does not.[48]

b) Other Federal Legislation

There were several other privacy-related bills introduced in 2019 and 2020 prior to the publication of this Review, including: Online Privacy Act of 2019,[49] Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data Act,[50] Do Not Track Act,[51] Social Media Privacy Protection and Consumer Rights Act of 2019,[52] Algorithmic Accountability Act of 2019,[53] Balancing the Rights of Web Surfers Equally and Responsibly Act of 2019,[54] Privacy Bill of Rights Act,[55] Information Transparency & Personal Data Control Act,[56] the DATA Privacy Act,[57] and the Preventing Real Online Threats Endangering Children Today ("PROTECT") Kids Act.[58] None, as of this writing, has gained significant traction.

Most of these bills substantially overlap with the comprehensive federal privacy bills discussed above—except for the following legislation:

- The Do Not Track Act, introduced by Senator Josh Hawley (R-MO), would require the FTC to develop an online Do Not Track ("DNT") system.[59] Opting in would prevent sites and apps from tracking a user without consent, but a user could still consent to tracking by certain apps or sites.[60] If a user opted in to DNT, then that user would transmit a signal indicating that a company would be disallowed from targeted advertising or information sharing without prior permission.[61] And in the event a user does *not* transmit such a signal, the site or app would still have to notify the user that the DNT system is available for them to opt into.[62]
- The Algorithmic Accountability Act of 2019, introduced by Senators Cory Booker (D-NJ) and Ron Wyden (D-OR), would require companies to conduct impact assessments to explain how their algorithms work and evaluate their algorithms' use of personal information against the following metrics: "accuracy, fairness, bias, discrimination, privacy and security."[63] Then, the Act would allow the FTC to promulgate compliance regulations based on the algorithm(s) used.[64]
- Two similar bipartisan bills, the Preventing Real Online Threats Endangering Children Today (PROTECT Kids Act),[65] introduced in the House by Representatives Tim Walberg (R-MI) and Bobby Rush (D-Ill.), and a set of amendments to the 1998 Children's Online Privacy Protection Act ("COPPA 2.0"),[66] introduced by Senators Ed Markey (D-MA) and Josh Hawley (R-MO), would update the original COPPA with additional protections. Both bills would raise the minimum age under which parental consent must be obtained before a company can collect personal data and location from 13 to 16 years old.[67] The PROTECT Kids Act would clarify that COPPA applies to mobile applications as well as other types of online activity, and expands the types of personal information protected under COPPA to include geolocation and biometric information.[68] COPPA 2.0, meanwhile, would provide parents with the ability to "erase" their children's data from particular services.[69]

B. Enforcement and Guidance

1. Federal Trade Commission

a) Priorities

In 2019, the Federal Trade Commission ("FTC") remained one of the most active and aggressive regulators of privacy and data security. The Commission continued to conduct policy reviews on a wide range of issues as part of its "Hearings Initiative" announced in 2018, which involved public hearings that took place through the spring of 2019.[70] The FTC also announced plans to study the privacy practices of internet service providers and has issued orders to seven companies to obtain information about their policies and practices with regard to collecting, using, and sharing personal information of consumers.[71] Relatedly, the FTC has also emphasized changes it has made to strengthen and improve "data security orders" issued to companies, making such orders more specific, increasing accountability for third-party assessors of compliance, and requiring that companies elevate data security concerns to their boards or similar governing bodies.[72]

The Commissioners emphasized their commitment to pursuing enforcement actions against companies that engage in unfair or unreasonable privacy and data security practices with all of the tools available to the FTC.[73] Recognizing potential limits to the FTC's authority, however, the majority of the Commissioners have called on Congress to enact legislation that would: (1) authorize the FTC to obtain civil penalties for initial privacy and data security violations; (2) provide the FTC with narrow Administrative Procedure Act ("APA") rulemaking authority to allow it to keep up with technological developments; and (3) give the FTC jurisdiction over nonprofits and common carriers.[74] The Commissioners also urged Congress to enact a national privacy law that would be enforceable by the FTC.[75] With growing public demand for additional consumer privacy protections, pressure on Congress to enhance the FTC's authority to protect consumer privacy will likely continue.

b) Data Security and Privacy Enforcement

Demonstrating the Commissioners' commitment to their cited priorities, the FTC continued to pursue enforcement actions related to privacy and data security in 2019, a number of which included significant monetary remedies and new prescriptive standards for information security and privacy programs in the technology industry.

Political Consulting Firm, Former CEO, and App Developer. In December 2019, the FTC entered into a settlement to resolve allegations that the former CEO of Cambridge Analytica and a developer of apps for the firm used deceptive tactics to collect personal information from social media users that it then used to target and profile voters.[76] Under the settlement agreement, the former CEO and app developer are prohibited from making false or deceptive statements about the extent to which they collect, use, share, or sell personal information and the purposes for which such data is acquired and distributed.[77] The former CEO and app developer are also required to destroy any personal information collected from consumers via the app that was used in violation of the FTC Act and any work product that originated from that data.[78] Notably, in its home country the firm has also been subject to discipline by the United Kingdom's Information Commissioner's Office for its data collection and utilization practices.[79]

The FTC also issued an opinion that found that the firm, which filed for bankruptcy last year, engaged in similar deceptive tactics in violation of the FTC Act and misrepresented its participation in the EU-U.S. Privacy Shield framework.[80] The final order prohibits the firm from misrepresenting the extent to which it protects personal information and its participation in the EU-U.S. Privacy Shield framework or other regulatory organizations.[81] The order also requires the firm to continue to apply Privacy Shield protections to personal information it collected while participating in the Privacy Shield program or to return and delete the information.[82]

Email Management Company. The FTC announced a final settlement with an email

management company in December 2019, resolving allegations that the company deceived consumers about how it accessed and used their email.[83] Specifically, the FTC alleged that despite telling consumers that it would not "touch" their personal emails while helping users consolidate emails or unsubscribe from unwanted communications, the company shared users' email receipts with its parent company, who in turn used the personal contact and purchasing information in the market research analytics products it sells.[84] Under the settlement agreement, the company is prohibited from misrepresenting the extent to which it collects, uses, stores, and shares consumer data.[85] Additionally, the company and its parent company must delete email receipts previously collected unless they obtain express consent to maintain the receipts.[86]

Operation Services Company. In November 2019, the FTC entered into a settlement with a Utah-based technology company that provides back-end operation services to multilevel marketers over allegations that the company failed to enact reasonable security safeguards, and, as a result, allowed a hacker to access personal information of approximately one million consumers over a two-year period.[87] Specifically, the FTC alleged that the company failed to delete personal information it no longer needed, neglected to implement cybersecurity safeguards to detect unusual activity on its network, and failed to adequately segment and test its network and conduct code review of its software.[88] Additionally, the FTC alleged that the company stored personal consumer information, including Social Security numbers, payment card information, and passwords, in clear, readable text on its network.[89] The proposed settlement prohibits the company from collecting, selling, sharing, or storing personal information unless it implements an adequate information security program which includes cybersecurity risk assessment, safeguards to protect personal information, and testing and monitoring of safeguards.[90] The settlement also requires a third-party assessment of the company's information security program every two years for the next 20 years.[91]

App Developer. In October 2019, the FTC pursued its first case against a the developer of a "stalking" app (an app that can allow purchasers to monitor a mobile device's activity without the knowledge or consent of the device's users). The FTC alleged such apps compromised the privacy and security of the mobile devices on which these apps were installed.[92] The developer allegedly failed to adequately secure the information collected from the mobile devices, which resulted in a hacker accessing usernames, passwords, text messages, GPS locations, photos, and other data.[93] The FTC alleged that the company and its owner violated the FTC Act and COPPA, which requires operators to secure information collected from children under the age of 13.[94] The settlement agreement requires the app developer and its owner to delete data collected from the apps and prohibits them from promoting, selling, or distributing any monitoring app that requires users to bypass a mobile device's security protections absent assurances that the app is being used for legitimate purposes.[95] It also requires the app developer and owner to implement and maintain a comprehensive security program and obtain third-party assessments of the program every two years for the next 20 years.[96] Under the settlement, the app developer and owner are also prohibited from violating COPPA and from misrepresenting the extent to which they protect the personal information they collect.[97]

Auto Dealer Software Company. Establishing a prescriptive standard for what constitutes reasonable security under the FTC Act, in September 2019 the FTC approved a final order settling charges against an Iowa-based auto dealer software provider that allegedly failed to take basic, low-cost measures to secure consumer data.[98] The FTC alleged that the security failures resulted in a data breach that exposed personal information of over 12 million consumers stored by 130 of the company's auto dealer clients.[99] Under the final order, the software company is prohibited from sharing, collecting, or maintaining personal information unless it implements and maintains a comprehensive information security program designed to protect consumers' personal information.[100] The order also requires the company to obtain third-party assessments of its information security program every two years for 20 years, and requires a senior corporate manager responsible for overseeing the information security program to certify

the company's compliance with the order on an annual basis.[101] Such a standard can be instructive for interpreting other privacy laws that do not define "reasonable security," including the CCPA (discussed further above).

Internet Search Engine and Video Sharing Platform. A web search engine and its subsidiary video sharing platform agreed to a settlement with the FTC and the New York Attorney General in September 2019 to resolve allegations that the video sharing platform collected personal information from children without parental consent, in violation of COPPA.[102] The video sharing service allegedly knew that a number of its channels were directed at children but did not comply with COPPA's requirements to obtain parental consent prior to collecting personal information about children.[103] As part of the settlement, the companies agreed to pay $34 million to New York and $136 million to the FTC, the largest monetary penalty the FTC has ever obtained in a COPPA case.[104] The proposed settlement also requires the companies to develop, implement, and maintain a system on the video sharing platform that allows channel owners to designate child-directed content so the companies can ensure compliance with COPPA.[105] Additionally, the settlement requires the companies to notify channel owners that child-directed content may be subject to COPPA and provide COPPA training to employees who interact with channel owners.[106] Finally, the settlement requires the companies to provide notice about their data collection practices and obtain parental consent prior to collecting personal information from children under the age of 13 and prohibits future violations of COPPA.[107]

Social Media Company. In July 2019, the FTC and DOJ filed a proposed consent order to resolve allegations that a social media company violated an earlier consent order with the FTC entered in 2012 by misrepresenting to consumers the extent of data sharing with third-party applications and the control consumers had over such sharing, and by failing to maintain a reasonable privacy program.[108] The FTC also alleged that the social media company engaged in deceptive practices related to the collection and use of consumer phone numbers to enable security features.[109] As part of the settlement, the company agreed to pay a $5 billion civil penalty, without admitting or denying the FTC's allegations except as specifically stated in the proposed order.[110] In addition to the monetary penalty, the settlement order expands on the privacy program requirements embodied in the 2012 order and enhances oversight and accountability of the company's data privacy practices.[111] In addition to requiring the company to implement early detection measures, the order also requires reporting of covered incidents to the FTC and regular status updates to the FTC regarding such incidents until their resolution.[112] The order further imposes the requirement that the company's chief executive periodically certify that the company is in compliance with its obligations under the order.[113]

Consumer Credit Reporting Agency. In July 2019, a consumer credit reporting agency agreed to pay at least $575 million, and up to $700 million total as part of a global settlement with consumers, the FTC, the Consumer Financial Protection Bureau, and attorneys general representing 50 U.S. states and territories based on allegations that the credit reporting agency's failure to implement basic measures to secure personal information on its network resulted in a data breach in 2017 that impacted 147 million people.[114] To address identity theft risks caused by the data breach, a portion of the settlement announced in July was to be dedicated to a fund that will provide affected consumers with credit monitoring services, a remedy discussed further below.[115] In addition to providing such monetary relief to consumers, the settlement also requires the credit reporting agency to implement a comprehensive data security program.[116] Under the settlement, the credit reporting agency must obtain third-party assessments of its information security program every two years for the next 20 years and must provide an annual update to the FTC regarding the status of the consumer claims process.[117]

Smart Home Products Manufacturer. The FTC entered into a settlement with a manufacturer of smart home products in July 2019 over allegations that the company misrepresented the measures it took to secure its wireless routers and internet-connected cameras, leaving sensitive consumer information, including live video and audio feeds,

exposed to third parties.[118] The manufacturer allegedly told consumers that its products offered "advanced network security," but failed to perform basic testing and remediation to address well-known security flaws and stored mobile app login credentials in clear, readable text on a user's mobile device.[119] Under the proposed settlement, the manufacturer is required to implement a comprehensive security program that includes specific planning, testing, and monitoring standards.[120] The settlement also requires the manufacturer to obtain biennial, third-party assessments of its software security program for ten years.[121]

Video Social Networking App. In February 2019, the operators of a video social networking app agreed to pay $5.7 million to settle FTC allegations that the company violated COPPA by collecting personal information from children without obtaining parental consent.[122] Profile information of users, including children, was public on the app and could be seen by other users,[123] and the FTC alleged that the company was aware that a significant portion of its users were under the age of 13 and had received thousands of complaints from parents of young children.[124] In addition to the monetary payment, the settlement requires the app's operators to take offline all videos made by children under the age of 13.[125]

Privacy Shield Enforcement. As discussed above, the FTC also brought actions against a number of companies regarding false claims of certification under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield frameworks, which allow companies to transfer personal data lawfully from the European Union and Switzerland, respectively, to the United States.[126] Each company held itself out as being certified and compliant with the Privacy Shield(s), despite failing to complete the certification process or allowing their certifications to lapse.[127] The FTC also sent warning letters to a number of other companies that falsely represented participation in these Privacy Shield frameworks, calling for them to remove statements regarding their participation in these frameworks from their websites and other company documents within 30 days.[128] The FTC has emphasized that enforcement of the Privacy Shield frameworks is a "high priority,"[129] and Gibson Dunn will continue to monitor developments in this area.

c) Circuit Split Over FTC Monetary Relief Authority

The FTC has long viewed its authority to recover monetary relief under Section 13(b) of the FTC Act as well settled, despite the lack of express reference to monetary remedy or relief in the provision, which refers only to "injunctions."[130] The United States Supreme Court had not yet addressed whether Section 13(b) authorizes monetary relief, but prior to this year, the nine federal courts of appeals that had addressed the issue had construed Section 13(b) to allow the FTC to obtain monetary relief, including restitution, rescission, and disgorgement.[131] However, in August 2019, the Court of Appeals for the Seventh Circuit issued a decision in *FTC v. Credit Bureau Center, LLC*, expressly overturning its own precedent and breaking with eight other circuit courts by holding that Section 13(b) does not authorize the FTC to seek monetary awards.[132]

The implications of *Credit Bureau* are potentially far-reaching. Other circuit courts may decide to reconsider their own opinions on this issue, many of which rely on a now-overturned Seventh Circuit decision. Additionally, in December, the FTC filed a petition for a writ of certiorari asking the Supreme Court to review the decision,[133] and the likelihood of the Supreme Court granting certiorari is heightened because the prior Seventh Circuit decision *Credit Bureau* overruled was relied upon by many other circuits in decisions upholding the FTC's authority to obtain monetary relief under Section 13(b). If the Supreme Court affirms the decision, the FTC's ability to obtain monetary relief under Section 13(b) will be eliminated or significantly restricted. In that case, the Commission, absent new statutory authority, would be limited to pursuing monetary remedies through other existing means, including the process set forth in Section 19 of the FTC Act that requires, as a condition to such relief, that the agency invoke a previously promulgated rule or prevail in a prior administrative proceeding. Unsurprisingly, while the Supreme

Court decides whether to grant certiorari, the Commissioners continue to urge Congress to pass legislation that will grant the FTC authority to obtain monetary relief for initial privacy and data security violations.[134] Congress's decision to pursue the legislation requested by the Commissioners may be influenced by the ultimate resolution of *Credit Bureau*.

2. Department of Health and Human Services and HIPAA

The Department of Health and Human Services ("HHS") continued in its efforts to enforce patient privacy protections in 2019, both through investigations and civil penalties for violations of Health Insurance Portability and Accountability Act ("HIPAA") regulations. HHS also continued to consider major overhauls to the HIPAA regulations. HHS was not the only entity to enforce healthcare privacy violations in the last year, as 2019 saw the resolution of the first multistate data breach lawsuit brought by Attorneys General of several states alleging violations of HIPAA. These developments are addressed below.

a) HHS OCR Enforcement

In February 2019, the HHS's Office for Civil Rights ("OCR"), the office that enforces HIPAA privacy, security, and breach notification rules, reported it had amassed a record $28.6 million in civil penalties from HIPAA violators in 2018.[135] In April 2019, OCR announced that it would reduce the penalties it seeks for lower-level HIPAA violations in the future,[136] and some observers have suggested that the total for 2019 was only around $12 million.[137] Nonetheless, there were several notable HIPAA-related settlements, judgments, and proceedings during 2019:

Medical Imaging Services Company. In May 2019, OCR announced a $3 million settlement with a medical imaging services company based on violations of HIPAA data privacy rules.[138] OCR found the imaging company had posted the PHI of more than 300,000 patients on an unsecured server, permitting search engines to index this PHI and make it publicly available.[139]

Hospital System. In October 2019, OCR reached a settlement imposing a civil penalty of more than $2.1 million on a hospital system after two hospital employees stole the PHI of more than 24,000 patients. An OCR investigation found the hospital system's compliance regime had failed to regularly review system access records, did not restrict employee authorization to appropriate levels, and did not timely report this breach to HHS.

State Government Health Agency. OCR announced in November 2019 that it would impose a $1.6 million civil penalty against a state agency which provides assisted living centers, drug and substance use services, and supplemental nutrition benefit programs. OCR found that a data breach led to the posting of roughly 6,500 patients' PHI on a publicly viewable internet site.[140] OCR also found that, because the agency did not deploy adequate activity audit controls, it was unable to determine how many unauthorized persons may have accessed the data at issue.

University Medical Center. Also in November 2019, OCR announced a settlement in which a university medical center agreed to pay penalties of $3 million and to take corrective action after PHI was impermissibly disclosed through the loss of two unencrypted mobile devices: a flash drive and a laptop.[141] OCR specifically noted that it had investigated the medical center for a very similar violation in 2010, and that the medical center continued to permit the use of unencrypted mobile devices even after this investigation.[142]

HIPAA Right of Access Initiative and Settlements. In spring 2019, OCR announced a new "HIPAA Right of Access Initiative" to enforce compliance with HIPAA requirements that guarantee patients' right to prompt and economical access to their health records.[143] Late in the year, OCR announced the first- and second-ever enforcement actions and settlements under this initiative. The first, announced in

September 2019, implicated a hospital operator that failed to timely provide a patient with access to her fetal heart monitor data.[144] The second, announced in December 2019, implicated a primary care provider that failed to timely provide a patient's electronic medical records to a third party.[145] In each case, the provider agreed to pay OCR $85,000 and to adopt a corrective action plan.[146]

Cancer Center Challenges OCR Authority. Finally, 2019 also saw litigation which might ultimately reduce OCR's regulatory capability going forward. In a 2018 ruling, OCR won a $4.3 million civil penalty against a hospital-based cancer center for violations of HIPAA. There, an administrative law judge for HHS found on summary judgment that the cancer center had violated HIPAA following the theft or loss of a laptop and two USB thumb drives containing unencrypted ePHI in 2012 and 2013, and assessed the penalty at issue.[147] In April 2019, however, the cancer center appealed this decision to a federal district court in Texas, requesting that the penalty be reduced or overturned. The cancer center's petition argues that the $4.3 million penalty was unconstitutionally excessive, and that OCR lacked statutory authority to impose it.[148] Gibson Dunn will continue to monitor developments on this matter.

b) Request for Public Comments on Reforming HIPAA

In addition to bringing enforcement actions, HHS also concluded a far-ranging review of HIPAA regulations, which sought to "remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and to promote the transformation to value-based healthcare, while preserving the privacy and security of PHI."[149] The request for public comments closed in February 2019 after receiving over 1,300 submissions,[150] with commenters ranging from state health agencies[151] and disability health advocates[152] to professional associations representing healthcare providers.[153] HHS has not yet announced further action on the proposed rulemaking, and Gibson Dunn will continue to monitor developments.

c) State Attorneys General Settle Multistate Action Premised on HIPAA

In a multistate data breach lawsuit alleging violations of HIPAA, a bipartisan group of 16 state Attorneys General, led by Indiana Attorney General Curtis T. Hill Jr., settled a lawsuit in Indiana federal court against a healthcare information technology company and its subsidiary related to a breach discovered in 2015 that compromised personal data of 3.9 million people.[154] The initial lawsuit, filed in December 2018, had alleged that the company failed to protect ePHI in the hands of its business associate after a breach related to a third-party web application.[155] Under the terms of the judgment and consent decree, the company agreed to pay a $900,000 settlement and to deploy more rigorous data security protections in the future.[156]

3. Securities and Exchange Commission

The Securities and Exchange Commission ("SEC") continued to devote increased attention to cybersecurity and data-protection issues in 2019, evidenced by its updated guidance on privacy and cybersecurity to private firms. One area of focus for the Commission has been cryptocurrency and initial coin offerings. While the SEC has continued to bring enforcement actions related to cryptocurrency, it has also suggested that it may refrain from taking action against virtual currency companies provided that certain parameters exist.

a) Data Privacy Guidance and Examination Priorities

In April 2019, the SEC issued guidance addressing privacy notices and safeguard policies

that SEC-registered investment bankers and broker-dealers must comply with.[157] This guidance noted that the SEC's Office of Compliance Inspection and Examination ("OCIE") had identified common deficiencies, such as failure to provide customers with sufficient data privacy notices or to inform them of their right to opt out of certain disclosures.[158] The guidance also noted that common areas of deficiency include use of personal devices to store customer information, use of unsecured networks, and failures to ensure that outside vendors adhere to confidentiality standards.[159]

Separately, OCIE released its 2020 Examination Priorities for registered firms in early January 2020.[160] The Priorities make clear that registrants' use of non-traditional sources of data from inputs like mobile device geolocations, consumer credit card records, and other internet-based information, sometimes known as "alternative data," will be a focus of examination review.[161] The Priorities also make clear that OCIE will prioritize cyber and other information security risks throughout its examinations.[162]

b) Cybersecurity and Data Breaches

Attempted Hacking of EDGAR database. In early 2019, the SEC brought charges against a Ukrainian-led group of nine defendants for attempting to hack the SEC's EDGAR[163] data system, the primary system through which companies submit filings required by law to the SEC. The defendants had hacked into the database to extract nonpublic information to use for illegal trading,[164] reaping an alleged $4.1 million in profits from the scheme.[165]

Data Misuse Risk Disclosure. The SEC also brought charges against a social network company alleging it had made misleading disclosures regarding the risk that the company might misuse consumer data. Specifically, the SEC alleged that the company failed to disclose that customer data had been misused for several years after the company became aware of the misuse. The SEC and the company agreed to settle the matter for a civil penalty of $100 million without the company admitting or denying the allegations.[166]

Enforcing Regulation Systems Compliance and Integrity. In September 2019, the SEC brought an enforcement action against a securities clearing agency for violation of the Regulation System Compliance and Integrity ("Reg SCI") rules, including failing to establish and enforce procedures around financial risk management and information system security. The clearing agency ultimately settled by agreeing to pay $20 million in penalties and to comply with extensive remedial measures.[167] The SEC noted that this action was particularly important in light of the risks that the clearing agency's practices posed to "the broader financial system."[168]

c) Cryptocurrency

Unregistered and/or Fraudulent Initial Coin Offerings. In 2019, the SEC focused substantial enforcement resources on combatting unregistered or fraudulent Initial Coin Offerings ("ICOs") to the public. In February, the SEC halted the unregistered sale of over $12.5 million in digital assets as part of an unregistered ICO. The SEC required the issuer to return funds to all investors who purchased the tokens and to register the tokens pursuant to the Securities Exchange Act of 1934. It did not, however, impose any monetary penalties, citing the issuer's cooperation and interest in taking prompt remedial steps.[169] In October, the SEC filed an emergency action and obtained a temporary restraining order against several offshore entities suspected of conducting an unregistered ICO that raised more than $1.7 billion of investor funds.[170] Finally, in December 2019, the SEC filed a complaint alleging a digital-asset entrepreneur had conducted a fraudulent ICO raising more than $42 million.[171]

First "No Action" Letter for Cryptocurrency. While continuing to target cryptocurrency operators who run afoul of federal regulations, the SEC also published its first ever "no action" letter for the use of a virtual token currency.[172] Specifically, the SEC stated that a

business-travel startup's sale of cryptocurrency travel tokens to the public would not trigger enforcement action, provided the token's price stays fixed at one U.S. dollar each, that they are used only for air charter services, and that the startup will not represent the tokens as having potential profit value.[173]

4. Other Federal Agencies

In addition to the FTC, HHS and SEC, other federal government entities continue to make headlines in the data security and privacy space. This past year, there were notable developments at the Federal Communications Commission ("FCC"), the Consumer Financial Protection Bureau ("CFPB"), the Department of Defense ("DoD"), and other federal agencies.

a) Federal Communications Commission

i. Illegal Robocall Mitigation

Mitigating and preventing illegal robocalls remained a core focus for the FCC in 2019. In June, the FCC issued rules clarifying that voice service providers could offer tools that blocked calls reasonably suspected to be illegal spam robocalls.[174] And in August, the FCC issued an order banning caller ID "spoofing" of phone numbers on text messages and on incoming international calls.[175]

Alongside these measures, the FCC continues to encourage telecommunications companies to roll out the STIR/SHAKEN[176] framework of call authentication for consumer use.[177] STIR/SHAKEN provides legitimate calls with digital authentication tokens, making it easier for carriers to identify and filter out spam robocalls. Several carriers have already adopted STIR/SHAKEN-based tools for users.[178] And under the newly passed federal TRACED Act[179], the FCC has increased authority to mandate other carriers to deploy such authentication.[180]

ii. National Security Purchasing Order and Proposed Rulemaking

In November, in response to purported concerns that Chinese telecommunications firms might be using technological assets to spy on the United States,[181] the FCC took two interrelated steps to bar recipients of FCC Universal Service Funds ("USF") from purchasing from foreign companies deemed to pose national cybersecurity threats. First, the FCC adopted an Order barring companies from spending any USF funds on such purchases.[182] At least one Chinese company alleged to present such a threat has sued the FCC to challenge this policy, and its petition is currently pending in the U.S. Court of Appeals for the Fifth Circuit.[183]

At the same time, the FCC issued a Further Notice of Proposed Rulemaking ("FNPR") seeking comment on rules that condition the receipt of *any* USF funds on certifying that a company does not use or purchase any such services or equipment.[184] The FNPR comment period closes on February 3, 2020, while the window for reply comments closes March 3, 2020.

b) Consumer Financial Protection Bureau

The CFPB has continued to operate under uncertainty regarding its continued existence and, by extension, its role in consumer data protection. Late in 2018, Kathy Kraninger was confirmed by the Senate as the new CFPB director.[185] Initially, she asserted the agency would engage in vigorous enforcement action and make consumer data security an important priority.[186] But in September 2019, Kraninger filed a Supreme Court brief

stating that she now believed the CFPB was unconstitutionally created and so must be disbanded.[187] The Court is set to decide that question in 2020.[188]

Despite this uncertainty, in July, the CFPB, in conjunction with the FTC and various state regulators, announced a settlement with a national provider of consumer credit information over a data breach which impacted 150 million consumers.[189] Under this agreement, the provider would pay up to $700 million in monetary relief, including up to $425 million in monetary relief to consumers.[190]

c) Department of Defense

The DoD made new efforts to address and defeat cybersecurity threats in 2019, particularly with respect to the national security supply chain. To this end, the DoD's Guidebook for Contractor Purchasing[191] highlighted that safeguarding DoD-covered defense information would be critical to supply chain management[192] and proposed various measures to check for vendor compliance with the Department's cybersecurity standards.[193]

Perhaps the most significant procurement-related developments came in the rollout of the DoD's Cybersecurity Maturity Model Certification ("CMMC") program for vendors on the DoD's supply chain. The CMMC will set out a proposed five-level hierarchy of "cyber hygiene" standards suppliers of DoD equipment must meet to contract with the Department, with each ascending level corresponding to a higher level of required protection depending on the sensitivity of the product involved.[194]

The CMMC's goal is to review and combine cybersecurity standards and best practices from across the information technology industry, to certify independent third-party organizations to conduct audits and inform the development of the standards, and to build upon existing vendor regulations by adding a verification component.[195] Throughout 2019, the DoD released draft versions of the CMMC for comment and review, with the most recent released in December.[196] As the CMMC program comes into place, vendors may face challenges implementing it and matching the new standards as they upgrade their measures of protection.[197]

DoD itself may also have some work to do: in 2019, various audits revealed areas of potential vulnerability which the DoD must work to address. In July, the DoD's Inspector General issued reports warning the Department had taken insufficient steps to verify the cybersecurity risk posed by off-the-rack technology systems purchased by DoD personnel,[198] and that DoD contractors failed to take cybersecurity precautions such as requiring multifactor authentication and systematically identifying network vulnerabilities.[199]

As it increases its focus on cybersecurity, the DoD will be guided by this year's iteration of the National Defense Authorization Act,[200] which establishes a Principal Cyber Advisor for each of the military services, directs the Department to produce an annual report on military cyberspace operations, and endorses the CMMC program.[201]

d) Other Agencies

Apart from these examples, other federal agencies also made news in the data and cybersecurity space throughout 2019. In June, the DOJ announced an antitrust investigation into some of the nation's largest technology companies,[202] with the company's practices of amassing substantial amounts of consumer data flagged as a potential antitrust concern.[203] Gibson Dunn will continue to monitor developments as this effort proceeds.

In September, the Commodity Futures Trading Commission imposed a $1.5 million fine on a commissions merchant for allowing an email phishing attack to steal $1 million in

customer funds via the company's computer systems.[204] In December, the Department of Commerce initiated a notice of proposed rulemaking on regulations to block transactions that might endanger the nation's information and communications technology supply chain.[205] 2019 also saw the Department of Energy continue efforts to improve the cybersecurity of America's critical infrastructure systems,[206] albeit with warnings from watchdogs like the Government Accountability Office that key vulnerabilities remained.[207] And the Department of Homeland Security ("DHS") itself came under scrutiny after a data breach at the Federal Emergency Management Agency ("FEMA") exposed the sensitive data of over 2.3 million disaster survivors.[208]

Notably, the National Institute of Standards and Technology ("NIST") also released two updated standards for other federal agencies to use in procurement when contracting with vendors. The first, NIST SP 800-171, Revision 2,[209] addresses contractual protections vendors should have when protecting Controlled Unclassified Information ("CUI"). This draft made comparatively minor changes from previous versions, but emphasized that Version 3, its next revision, will likely provide a comprehensive update.[210] NIST also released a draft of NIST SP 800-171B,[211] a heightened set of contracting standards intended for vendors engaged in "Critical Programs and High Value Assets," and specifically focused on "(1) penetration resistant architecture; (2) damage-limiting operations; and (3) designing for cyber resiliency and survivability."[212] And in January of 2020, NIST also released Privacy Framework Version 1.0, aimed at providing voluntary strategies and tools for organizations that want to "improve their approach to using and protecting personal data."[213]

As data and privacy concerns become more salient, the depth and degree of federal agency involvement will surely continue to grow.

5. State Attorneys General and Other State Agencies

State-level regulators also continued to play a key role in data privacy and security matters in 2019, collaborating to bring enforcement actions yielding recoveries in the hundreds of millions of dollars and actively protecting consumers from the danger of data breaches.

a) State Attorneys General

As noted above, in July 2019, Attorneys General from 48 states, Puerto Rico, and the District of Columbia, along with the FTC and CFPB, settled a long-running dispute against a major credit reporting agency. This action stemmed from a 2017 data breach in which unauthorized persons gained access to portions of the reporting agency's network, affecting more than 147 million consumers. Under the settlement, as discussed, the reporting agency is required to implement various consumer protection safeguards and controls and to offer no-cost credit monitoring to consumers as discussed above. In particular, in addition to other remedies described above, the agency had to pay the Attorneys General $175 million for purposes including consumer education and litigation costs.[214]

On July 31, a manufacturer of security camera software agreed to pay $8.6 million to settle multistate litigation alleging that the company violated the False Claims Act ("FCA") and state whistleblower acts because it knowingly failed to report or remedy flaws in the security surveillance systems it sold to the federal government and to multiple state governments. These flaws made the system vulnerable to hackers. The settlement provided refunds to the federal government and 16 states that had purchased the allegedly defective software. This was the first cybersecurity-related settlement under the FCA or comparable state statutes.[215]

In October 2019, the Attorneys General of 47 states and territories announced a multistate antitrust investigation into a social networking platform. This investigation is being led by the New York Attorney General and will focus on whether the platform has stifled

competition and put consumers' data at risk. Many of the Attorneys General who have joined this investigation have issued statements emphasizing the need to combat anticompetitive business practices and protect consumer data.[216]

Individual states also took action apart from litigation. In October 2019, New Jersey's Attorney General announced a new "Cyber Savvy Youth" initiative. This initiative will educate and test the cybersecurity knowledge of students from kindergarten through high school. At the same time, the state's Division of Consumer Affairs announced the 2018 statistics regarding data breaches affecting New Jersey residents: 906 data breaches were reported to the New Jersey State Police last year, a nearly 6 percent decrease from the 958 breaches reported in 2017. In addition, civil settlements reached by the Attorney General's Office following data breach incidents had resulted in more than $6.4 million in recoveries for the state on a year-to-date basis.[217]

b) New York Department of Financial Services

Apart from Attorneys General, other state regulators continued to engage in the data privacy space. In May 2019, for example, New York's Department of Financial Services ("DFS") announced the creation of a new Cybersecurity Division. The Division will focus on protecting consumers and industries from cyber threats by conducting cyber-related investigations, issuing regulatory guidance, offering counsel, and enforcing DFS's cybersecurity regulations.[218]

II. Civil Litigation

A. Data Breach Litigation

1. High-Profile Incidents and Related Litigation in 2019

Just nine months into the year, the number and sheer scale of cyberattacks occurring in 2019 had already surpassed those of prior years, earning 2019 the label of "the worst year on record" for data security breaches.[219] Not surprisingly, several high-profile attacks in 2019, including the following, culminated in consumer class action and shareholder litigation.

Clinical Laboratories. On June 3, 2019, a medical diagnostics provider announced that its medical billing contractor suffered a data breach between August 1, 2018 and March 30, 2019, in which hackers accessed the personal data of nearly 12 million of the laboratory's customers.[220] Another leading clinical laboratory that contracted with the same billing contractor was also impacted by the breach, which affected up to 7.7 million of its patients.[221] Class action lawsuits were subsequently filed in federal and state courts, including in California and New Jersey.[222] On June 18, 2019, the billing contractor filed for bankruptcy, citing the fallout from the breach.[223]

Convenience Store Chain. On December 19, 2019, a convenience store chain announced that it had discovered malware capable of exposing credit card numbers, expiration dates, and cardholder names at all of the chain's more than 850 stores.[224] In the weeks following the announcement, nearly a dozen proposed class action lawsuits were filed in the Eastern District of Pennsylvania.[225]

2. Updates in High-Profile Data Breach Cases from Prior Years

a) Key Settlements

Consumer Credit Reporting Agency. As outlined above, in July 2019 a consumer credit reporting agency agreed to pay at least $575 million, and up to $700 million, as part of a global settlement with consumers, the FTC, the Consumer Financial Protection Bureau, and 50 U.S. states and territories based on allegations that the reporting agency's failure to implement basic measures to secure personal information on its network resulted in a data breach in 2017 that impacted 147 million people. On December 19, 2019, a federal district judge in Georgia granted final approval to that portion of the global settlement defining monetary relief for consumers impacted by the breach. Under approved settlement, the reporting agency will pay up to $425 million in restitution to consumers, $77.5 million in attorney's fees to class counsel, and up to $3 million in class counsel litigation expenses.[226] The company also agreed to spend $1 billion to improve its own cybersecurity, pay in full all valid consumer claims for out-of-pocket expenses, and cover credit monitoring services for affected consumers.[227] The federal judge approving the consumer settlement concluded that the deal, which encompasses more than $7 billion in aggregate benefits to consumers, represents "the largest and most comprehensive recovery in a data breach case in U.S. history by several orders of magnitude."[228]

Internet Service Company. On July 20, 2019, a federal district judge in the Northern District of California preliminarily approved a $117.5 million settlement to resolve litigation arising out of a trio of data breaches of an internet service provider's user account data between 2012 and 2016.[229] The deal covers an estimated 194 million class members.[230] The preliminary approval came after the judge had rejected prior versions of the settlement, citing a lack of sufficient specificity as to the class size, monetary and non-monetary relief, and details of the nature of the data breaches.[231]

Earlier in the year, in January 2019, a California Superior Court judge approved a $29 million deal to resolve three shareholder derivative lawsuits against the company's former officers and directors in California and Delaware, which arose out of the same series of data breaches.[232]

b) Litigation

Social Media Company. Following reports that Cambridge Analytica obtained information on a social media company's users, the social media company faced several shareholder derivative lawsuits and consumer class actions, the latter of which were ultimately consolidated in the Northern District of California. On September 9, 2019, the federal district judge presiding over the consumer class actions permitted certain of the plaintiffs' claims to proceed, while granting the social media company's motion to dismiss other claims.[233] The court held, with respect to the surviving claims, that plaintiffs maintained a privacy interest in information they disclosed to a limited audience and that they had alleged an injury sufficient to confer standing based on that privacy interest alone, even in the absence of a secondary economic injury such as identity theft.[234] On October 31, 2019, the court issued a single-sentence order denying the social media company's motion to certify the court's Article III standing analysis for interlocutory review.[235] A hearing on class certification is scheduled for late 2021.[236]

Sports Apparel Company. Last year we also reported on class action litigation filed against a fitness apparel company following its announcement that hackers obtained access to the data of 150 million users of its fitness-tracking app.[237] On February 11, 2019, a federal district judge in the Central District of California granted the company's motion to compel arbitration, holding that by clicking "accept" in response to the app's terms and conditions, which incorporated the American Arbitration Association Rules, the plaintiff had "clearly and unmistakably delegated the arbitrability issue to the arbitration."[238]

3. The Deepening Circuit Split on Standing Post-*Spokeo*

In 2019, the divide among circuit courts over the requirements for Article III standing in

data breach cases continued to deepen in the wake of the Supreme Court's 2016 ruling in *Spokeo, Inc. v. Robins*.[239]

In *Spokeo*, the Supreme Court held that a statutory violation alone cannot establish injury-in-fact standing; a plaintiff must allege a "concrete" injury stemming from the violation.[240] Following that decision, lower courts have diverged over what facts a plaintiff must allege to establish a "concrete" injury sufficient to confer Article III standing in data breach cases. While some courts of appeals, including the Ninth and D.C. Circuits, have held that the theft of consumers' private information in and of itself establishes a "substantial risk" of future harm sufficient to confer standing,[241] other courts, including the Fourth and Eighth Circuits, have held that such allegations are too speculative.[242]

In June 2019, a divided panel of the D.C. Circuit reaffirmed the split, holding that government employees "cleared the low bar to establish standing" by alleging that they faced an increased risk of identity theft following a 2015 hack of the Office of Personnel Management ("OPM").[243] The majority's decision expanded on the court's prior holding in *Attias v. CareFirst*, which had pointed to the circumstances of the breach at issue to conclude that the hackers had "the intent and the ability to use" the stolen data "for ill."[244] Here, the majority reasoned, the sensitivity of the stolen data and the fact that some class members had already suffered identity theft or fraud rendered the question of the hacker's intent "markedly less important."[245] The majority further rejected the dissent's conclusion that the passage of two years between the cyberattacks and the filing of the complaint "was enough to render the threat of future harm insubstantial."[246]

Thus far, the Supreme Court has not signaled an interest in resolving the divide. As we reported last year, the Supreme Court denied a petition to review the D.C. Circuit's *Attias* decision.[247] In March 2019, the Supreme Court again passed on the opportunity, declining to review the Ninth Circuit's decision in *In re Zappos.com, Inc.*, which held that plaintiffs had established standing based on the allegation that the information exposed in a data breach could be used to cause future harm.[248]

B. Telephone Consumer Protection Act Litigation

The past year brought several significant actions and noteworthy developments related to the Telephone Consumer Protection Act ("TCPA").

First, at the start of the year, the FCC's Consumer and Government Affairs Bureau solicited comments on a motor vehicle servicer's petition for declaratory review around the FCC's understanding of "dual purpose" communications (communications that both provide a service and simultaneously act as commercial messages for TCPA purposes).[249] The servicer argued its prerecorded messages to customers, recommending that they take their cars for inspections at certain times, were not "dual purpose," since the communications allegedly were entirely service-based rather than commercial.[250] Accordingly, the servicer argued, the communications should not be subject to the heightened written consent standards the TCPA imposes on commercial messages.[251] The FCC has yet to issue guidance in response to the petition, but Gibson Dunn will continue to monitor developments in this area, and the Commission's interest in such questions suggests clarifications of the "dual purpose" concept might be made in 2020.

Turning to another aspect of the TCPA, as discussed above, on June 6, the FCC adopted a Declaratory Ruling and Third Further Proposed Rulemaking to allow phone carriers to block both illegal and unwanted robocalls by default without waiting for customers to opt in to the service.[252] The FCC's ruling requires carriers to use "reasonable analytics"—such as those used by call-management apps—to determine which calls to block.[253]

On June 20, the Supreme Court issued an opinion in *PDR Network, LLC v. Carlton & Harris Chiropractic, Inc.*, although the Court did not definitively decide the issue presented.[254] Acknowledging that it is "difficult to answer [the] question" of whether the Hobbs Act requires the district court to accept the FCC's legal interpretation of the term "unsolicited advertisement" in the TCPA, the Court remanded to the Fourth Circuit to answer two preliminary questions: first, whether the FCC's 2006 order is a "legislative" or "interpretive" rule under the APA, as the former has the "force and effect of law" while the latter does not;[255] and second, whether PDR Network had a "prior" and "adequate" opportunity to seek judicial review of the FCC's 2006 order, as required by Section 703 of the APA.[256] If not, the Court noted that PDR Network "may" be permitted to challenge the validity of the order under the APA, even if the order is deemed a legislative rather than an interpretive rule.[257] In a four-Justice concurrence, Justice Kavanaugh deemed the question "straightforward," stating that the relevant statute does not "expressly preclude judicial review of an agency's statutory interpretation in an enforcement action" and PDR Network therefore "may argue to the District Court that the FCC's interpretation of the TCPA is wrong," and he concluded that, on remand, "the District Court should interpret the TCPA under usual principles of statutory interpretation, affording appropriate respect to the [FCC's] interpretation."[258] He went on to provide an extensive analysis that will "remain[] available to the court on remand . . . and . . . to other courts in the future."[259]

In August, the Eleventh Circuit created a circuit split when it concluded that the receipt of a single unsolicited text message—which is "more akin to walking down a busy sidewalk and having a flyer briefly waived in one's face"—does not generate the harm necessary to give rise to claims under the TCPA.[260] That ruling is at odds with the Ninth Circuit's January 2017 decision in *Van Patten v. Vertical Fitness Group, LLC*, which held that the receipt of just two unsolicited text messages constituted concrete harm under Article III.[261] Though no parties have filed petitions for certiorari to date, it is likely that the Supreme Court will be presented with the question of what constitutes standing under the TCPA.

Later in the year, within a 15-day span a social media company and a communications company filed separate petitions for certiorari with the Supreme Court regarding the constitutionality of the TCPA. Specifically, the companies are asking the Court to opine on whether the TCPA's prohibition on calls made using an automated telephone dialing system ("ATDS") or an artificial or prerecorded voice is an unconstitutional restriction on speech.[262] The social media company's petition also asks the Court whether the Ninth Circuit's statutory interpretation of the TCPA's definition of an ATDS in *Marks v. Crunch San Diego*[263] is overly broad.[264] Although the FCC sought public comments on this question following both *Marks* and the D.C. Circuit Court's decision in *ACA International v. FCC*,[265] the agency has yet to issue any guidance. Thus, the Supreme Court's consideration of this question would be significant. And in a further constitutional challenge to the TCPA, this January the Supreme Court granted certiorari in *Barr v. American Association of Political Consultants Inc.*,[266] in which it will consider whether the TCPA's "government-debt exception" violates the First Amendment and, if so, whether the appropriate remedy would be to sever the exception from the statute.

Finally, on December 30, President Trump signed into law the Telephone Robocall Abuse Criminal Enforcement and Deterrence ("TRACED") Act, which is intended to combat illegal robocalls under the TCPA.[267] Specifically, the legislation: (1) increases civil penalties for TCPA violations to up to $10,000 per call; (2) provides the FCC with additional time to bring actions based on violations related to knowingly providing misleading or inaccurate caller ID information; and (3) requires telecommunications carriers to implement, at no additional charge, the FCC's STIR/SHAKEN call authentication procedures to prevent scammers from spoofing numbers.[268] The House in July passed a similar law aimed at cracking down on unwanted automated phone calls, the Stopping Bad Robocalls Act, on which the Senate has yet to vote.[269]

C. Biometric Information Privacy Act Litigation

As we foreshadowed in last year's Review, 2019 was an active year for biometric privacy litigation. In particular, litigation continued around Illinois' Biometric Information Privacy Act ("BIPA"), which confers a private right of action to individuals "aggrieved" under the statute,[270] unlike similar statutes in states such as California, Texas, and Washington. The Illinois Supreme Court seemed to invite such litigation with its decision in *Rosenbach v. Six Flags*,[271] in which the court held that individuals aggrieved under the BIPA have standing to sue without alleging an actual injury, because the BIPA provides individuals with a substantive right to control their biometric information and no-injury BIPA violations are not merely "technicalit[ies]" but instead are "real and significant" harms to important rights.[272]

As a result of *Rosenbach*, to withstand a motion to dismiss plaintiffs need merely to allege that they are aggrieved persons under the BIPA. Illinois courts and federal courts applying Illinois law have applied *Rosenbach* in precisely this manner. For example, in *Rottner v. Palm Beach Tan, Inc.*, an Illinois appellate court reversed the lower court's dismissal of a BIPA action for failure to sufficiently plead damages, issued prior to *Rosenbach*, because "Rottner, like Rosenbach, has standing to sue and has adequately stated a claim for liquidated damages under section 20 of the Act, even if she has alleged only a violation of the Act and not any actual damages beyond violation of law."[273] Similarly, in *Rogers v. CSX Intermodal Terminals, Inc.*, the U.S. District Court for the Northern District of Illinois granted in part the defendant's motion to dismiss putative class action claims for intentional and reckless violations of the BIPA, which the court deemed insufficiently pled, but it denied the motion as to claims of statutory violations of the BIPA, which the court noted required only that a plaintiff allege he or she was an aggrieved person under the BIPA.[274] Likewise, in *Namuwonge v. Kronos, Inc.*,[275] the court determined that the plaintiff failed to plead any facts that would support a finding of intentionality or recklessness, and instead merely alleged that the putative class was composed of aggrieved persons under the BIPA.[276] The court thus struck the intentional and reckless claims from the complaint, but it left untouched the remaining BIPA claims.[277]

In addition to using *Rosenbach* to defeat motions to dismiss, plaintiffs also have used it to avoid being compelled into arbitration. In *Liu v. Four Seasons Hotel, Ltd.*,[278] an Illinois appellate court rejected the defendant's attempt to compel arbitration of its employees' BIPA claims on the ground that the claims merely sought "wages and hours" relief, clarifying that: "[s]imply because an employer opts to use biometric data, like fingerprints, for timekeeping purposes does not transform a complaint into a wages or hours claim."[279] Although this holding applies narrowly to circumstances in which employers attempt to construe privacy claims as wage and hour claims, it nevertheless highlights *Rosenbach*'s impact in facilitating the survival of such claims. Indeed, some companies are choosing to settle BIPA claims for sizeable sums rather than litigate them, as Smith Senior Living and its timekeeping company Kronos (which lost a motion to dismiss in a separate BIPA action last year) did to the tune of $1.55 million for a class of just under 1,700.[280]

Perhaps the biggest impact of *Rosenbach*, though, has been the flood of class actions filed against large corporations as a result of the BIPA's relatively simple pleading requirements.[281] As this Review went to press, the Supreme Court declined to grant certiorari on one closely watched case in this area.[282] The case involves the Ninth Circuit's affirmance of the certification of a class of a social media company's users for alleged violations of the Illinois BIPA predicated on the company's use of facial recognition technology.[283]

D. Other Notable Cases

In addition to the cases described above, 2019 brought developments in a number of matters discussed in last year's Review, as well as a host of new matters concerning shareholders' derivative rights, companies' recordation and storage of data through connected devices and otherwise, the Internet of Things, medical records, the scope of the

Wiretap Act, and privacy?related insurance coverage. We describe some of the key updates and cases on these issues in greater detail below.

Social Media Company. As highlighted in last year's Review, at the end of 2018, the media reported that two bugs had exposed profile data of millions of users of a social media service.[284] Upon release of the news, plaintiffs filed complaints, which were consolidated in a single class action complaint in the Northern District of California.[285] The company filed a motion to dismiss the complaint on April 10, 2019, but later agreed to a settlement in principle after mediation on August 14, 2019.[286] Under the proposed settlement, the company must pay $7.5 million; individual claimants will each receive up to $5.00, with the potential to receive up to $12.00 depending on the number of claimants.[287]

Derivative shareholder litigation against the social media company, also discussed in last year's Review, was also consolidated in the Northern District of California. In May 2019, the company moved to dismiss the shareholders' amended complaint, arguing, among other things, that it fixed the bug before it made any statements shareholders claimed were "misleading," and that shareholders had failed to adequately plead scienter or material harm to the business.[288] The court has yet to rule on the motion to dismiss.

Social Media Company. After the media reported in March 2018 that Cambridge Analytica had obtained information on some of a different social media company's users, the social media company's shareholders brought a number of derivative lawsuits that were consolidated in the U.S. District Court for the Northern District of California. On March 22, 2019, the court granted in part the company's motion to dismiss the shareholders' state claims on *forum non conveniens* grounds, finding the forum selection clause in the company's Restated Certificate of Incorporation valid and applicable.[289] The court granted the social media company's motion to dismiss the federal claims with leave to amend, holding that the shareholders failed to adequately plead demand futility.[290] The shareholders filed an amended complaint on December 17, 2019.[291]

In May 2019, the Washington, D.C. Superior Court denied the company's motion to dismiss claims brought by the D.C. Attorney General alleging violations of the D.C. Consumer Protection Procedures Act for failing to take reasonable steps to protect the "trove" of personal consumer data that the company "collects and maintains."[292] The court concluded that the Attorney General had adequately pleaded the merits of its case at the motion-to-dismiss stage and any existing factual questions should be decided by a jury.[293]

Banking Institutions. In last year's Review, we reported on litigation against banking institutions claiming that the institutions impermissibly recorded consumer calls. In February 2019, the U.S. District Court for the Western District of Pennsylvania approved a stipulated dismissal of one such action following a settlement between the bank and the plaintiff.[294] It does not appear that the institution involved in the California-based case has appealed from the California Court of Appeals' decision, which reversed summary judgment for the institution and held that the institution had failed to show it lacked intent to record the relevant conversations, defining "intent" as acting with "the purpose or desire of recording a confidential conversation, or with the knowledge to a substantial certainty" that a confidential conversation will be recorded.[295]

Technology Company - Location History. On December 19, 2019, the Northern District of California granted a technology company's motion to dismiss class-action claims that it had stored users' locations even where those users had turned off location history settings in apps.[296] The plaintiffs had asserted claims under the California Invasion of Privacy Act ("CIPA") and California's state-constitutional right to privacy.[297] In its motion filed in May 2019, the company argued that the plaintiffs had consented to the collection and storage of location data by agreeing to its Privacy Policy, and that the laws plaintiffs cited were inapplicable because the company did not deploy an "electronic tracking device" "attached to a . . . movable thing" under the CIPA or egregiously breach social

norms under the state constitution.[298] The court found the statements within the company's Privacy Policy and Terms of Service irrelevant, but it concluded, among other things, that the CIPA applies only to "unconsented geolocation tracking," not the storage and collection of geolocation data, and that the plain terms of the statute did not encompass the circumstances presented.[299] The court therefore dismissed the plaintiffs' CIPA claims with prejudice.[300] The court also found that the plaintiffs had failed to plead facts to establish a legally protected privacy interest under the state constitution, but granted plaintiffs leave to amend the complaint on this issue.[301]

Technology Company - Medical Records. On June 26, 2019, plaintiffs filed a class action complaint and demand for jury trial against a technology company and a private university, claiming that the university turned over to the company "the confidential, highly sensitive and HIPAA-protected records of every patient who walked through its doors between 2009 and 2016" without notifying patients or obtaining their express consent, thereby violating state consumer fraud, contract, intrusion upon seclusion, and unjust enrichment laws.[302] The plaintiffs labeled the company's and the university's assertions that the medical records were de-identified "incredibly misleading," alleging that the records contained detailed date stamps and free-text notes, and that because the company is a "prolific data mining" company, it could determine individuals' identities from the records.[303] The plaintiffs further claimed that the company collected the records in order to build and patent its own commercial electronic health record system and develop software that could be sold at premium prices, and that, in exchange for providing the records, the university received a perpetual license to use the software that the company developed.[304] The university and company filed separate motions to dismiss, arguing, among other things, that the plaintiffs had failed to allege an actual injury and thus lacked Article III standing.[305] The motions are currently pending.

Connected Vehicles and Devices, and the Internet of Things. On November 11, 2019, an automobile manufacturer we discussed in last year's Review moved to decertify state-based classes of drivers in Michigan, Illinois, and Missouri,[306] following the U.S. Supreme Court's refusal in January to hear the manufacturer's challenge to the certifications.[307] Also on November 11, the manufacturer moved both for summary judgment on the drivers' claims that defects in certain vehicles' infotainment systems made the vehicles vulnerable to hackers and to dismiss the claims for lack of subject matter jurisdiction.[308] The manufacturer asserted that none of the plaintiffs had alleged that his or her vehicle's system had malfunctioned or was hacked; thus, the plaintiffs had suffered no legally cognizable injury.[309] It also argued that there is a growing consensus among courts that consumers' claims that they "overpaid" for a product because it theoretically could have been made safer are insufficient to establish subject matter jurisdiction.[310] The court has yet to rule on these dispositive motions.

Additional connected-device cases continue to emerge, and the bases of such cases continued to test the scope of the Wiretap Act in 2019. In May, for example, the Northern District of California held that the vibration intensity settings a user chooses on an adult product constitutes "content" under the Wiretap Act, and the harvesting of such data could constitute intrusion upon seclusion under California state law.[311] In August, the U.S. District Court for the District of New Jersey partially granted two electronic companies' motion-to dismiss claims that Smart TVs collected data on consumers, including which programs consumers watched, IP and MAC addresses, and ZIP codes, and that the companies sold the data to third parties who used it to conduct targeted advertising.[312] The court dismissed the plaintiffs' state law claims and claims under the Video Privacy Protection Act ("VPPA"), finding the latter "squarely foreclosed" by controlling precedent that established such "static" identifying information does not constitute personally identifiable information under the VPPA.[313] The court allowed the plaintiffs' Wiretap Act claim to go forward, finding that the companies were not parties to any allegedly intercepted "communication" between the content provider and the Smart TV, and that information about what consumers are watching constitutes "content" under the Act.[314] The companies have asked the court to reconsider its ruling on the Wiretap Act claim, or, in the alternative, to certify the court's order for interlocutory appeal.[315]

In June, plaintiffs filed class action complaints in California state court (subsequently removed to federal court) and Washington federal court against a large retailer and technology company, alleging that the company used voice-enabled devices to build a "massive database of billions of voice recordings" containing private personal details of children, among others, without the consent of the children or their parents.[316] The plaintiffs claimed that the company does not have to store these voice recordings but does so for its own commercial gain, and they asserted that the company's alleged actions violate multiple states' wiretap laws.[317] Since filing, some plaintiffs have voluntarily dismissed their complaints without prejudice.[318] The company moved to dismiss the remaining plaintiffs' claims in early January 2020, arguing that the plaintiffs had failed to state a claim because, among other things, the "mere creation of recordings within a communication service" intended to provide instructions over the internet does not constitute illicit interception, eavesdropping, or recording.[319]

Minors' privacy rights also were in the news in 2019 as a result of class actions filed against app developers and major media companies alleging that the defendants used gaming apps for children to track online behavior and leveraged the collected data to target advertising to the children playing the games.[320] On May 22, 2019, the Northern District of California allowed the majority of the plaintiffs' privacy claims to move forward, finding, among other things, that the plaintiffs' allegations that defendants gathered user-specific information, worked with third-party companies to buy and sell the information, targeted ads to users, and tracked users' responses to those ads met the standard required to survive a motion to dismiss.[321] Trial is currently scheduled for October 2020.[322]

Computer Fraud and Abuse Act Litigation. In July, an online ticket vendor reached a favorable settlement on its allegations that individuals had used bots to purchase large quantities of tickets in violation of the company's Terms of Use, as we described in last year's Review. Under the settlement, the defendants are permanently enjoined from using the ticket vendor to search for or purchase tickets, from violating the vendor's Terms of Use, and from conspiring with others to engage in such activities, among other things.[323]

Cybersecurity Insurance and Acts of War. In December 2019, an insurer, about which we wrote in last year's Review, settled with its insured after the latter filed an appeal in the Eleventh Circuit challenging a district court decision that the insured's personal injury policy did not cover data breach litigation costs.[324] Similarly, the bank and insurer we discussed in last year's Review in the context of financial institution bonds also settled in March 2019.[325]

In a case that could have broad implications for companies seeking to insure themselves against cybersecurity attacks, a suit between a food and beverage company and its insurer after the insurer denied coverage for a ransomware attack was one of the most salient of 2019.[326] The food and beverage company was one of hundreds of companies impacted by the "NotPetya" cyberstrike in 2017, for which the U.S. government ultimately assigned responsibility to Russia.[327] When the company made a claim to its insurance company to cover costs resulting from the attack, pointing to provisions of its insurance policy that provided coverage for damage to electronic data or damages resulting from the failure of electronic data processing equipment or media, the insurance company invoked an exception to coverage for "hostile or warlike action in time of peace or war."[328] The food and beverage company has asserted breach of contract, promissory estoppel, and unreasonable conduct claims under Illinois law and has requested at least $100 million in damages.[329] A pharmaceutical company filed a similar suit against its insurer in New Jersey related to the NotPetya strike, seeking $1.3 billion in damages.[330] Neither case has yet resolved, but as the risks and prevalence of cybersecurity attacks increase, in particular attacks with suspected connections to foreign governments, the interpretation of "act of war" exclusions in security-related insurance policies likely will become increasingly important.

Cy Pres *Settlements*. An open question going into 2020 is the legality of *cy pres*-only settlements, or settlements from which the proceeds go to public interest organizations rather than class members, which we discussed in last year's Review. Although the Supreme Court seemed poised to address this question in *Frank v. Gaos*,[331] a case concerning a technology company's alleged transmission of users' search terms to third parties through referrer headers, the Court instead remanded the case to the district court to evaluate the plaintiffs' standing in light of *Spokeo, Inc. v. Robins*,[332] discussed above.

III. Government Data Collection

A. Collection of Data from Computers, Cellphones, and Other Devices

This year, a number of court decisions addressed the issue of individuals' privacy rights with respect to data stored on cell phones and other personal electronic devices. Although one of the more prominent decisions bolstered such rights by narrowing the Government's ability to collect and search data without warrants, courts have reached divergent conclusions regarding the Government's authority to demand that an individual provide biometric input (such as pressing their fingerprint) to unlock digital devices.

In November 2019, a federal district court in Massachusetts held that the Fourth Amendment prevented warrantless data searches of electronic devices at border crossings unless there is reasonable suspicion the devices contain contraband.[333] In doing so, the court cabined the Fourth Amendment's traditional "border search exception," under which a variety of suspicionless searches are permitted.[334] The court found that while that exception might allow for cursory searches—such as taking a brief look to determine whether a device is in fact owned by the person carrying it—it did not extend to a full search of one's personal photographs, phone contacts, or sensitive personal or professional data.[335] Both parties have appealed the decision to the U.S. Court of Appeals for the First Circuit, where the matter is pending.[336]

As digital devices increasingly require thumbprint or facial recognition credentials upon startup, a split has emerged over whether the Government can compel arrestees to provide their biometric inputs to unlock their devices.

In the *Matter of the Search of a Residence in Oakland*, prosecutors applied for a warrant to search electronic devices in an extortion investigation.[337] The warrant application sought the authority to compel any person present during the search to provide biometric inputs (such as pressing a finger or displaying their face) to unlock the devices.[338] The court rejected the application, reasoning that providing biometric data is akin to compelling a witness to provide testimony, and thus a violation of the Fifth Amendment. In reaching this conclusion, the Court analogized forced biometric authorization to forcing a witness to produce a passcode to a digital device, which courts have regularly found to invoke the Fifth Amendment privilege.[339]

In *United States v. Barrera*, however, a federal court in Illinois reached the opposite result.[340] The court in *Barrera* found the Fifth Amendment is invoked only when "the compelled act forces an individual to disclose the contents of the subject's own mind," and is distinct from one's physical characteristics.[341] In this respect, the *Barrera* Court compared compelled biometric use to physical acts, such as providing blood samples or handwriting exemplars, which courts have routinely held to be non-testimonial in

nature.[342]

B. Other Notable Developments

1. Extraterritoriality and Warrants

In 2018, Congress passed the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act").[343] The Act's two main prongs were to: (1) empower the government to make agreements with foreign countries that mutually remove any barriers to compliance with each nation's court orders to produce data; and (2) clarify that any communication provider subject to U.S. jurisdiction must, upon appropriate legal request, produce any data in their possession, regardless of where the data is stored.[344]

This year saw the United States and the United Kingdom sign the first-ever CLOUD Act bilateral pact: the US-UK Bilateral Data Access Agreement.[345] Under the agreement, the U.S. can now access any electronic data stored in the United Kingdom using American legal processes (and vice versa).[346] However, the agreement has brought protest from groups who believe that standards for search and seizure in the United Kingdom are weaker than those required by the Fourth Amendment, putting civil liberties at risk.[347]

Apart from its United Kingdom agreement, the federal government has also begun talks with both the European Union[348] and Australia,[349] suggesting 2020 may well bring new CLOUD Act pacts.

This year the government also sought to clarify the scope of the CLOUD Act via formal Department of Justice guidance. The DOJ's white paper asserted that the second, location-based prong of the CLOUD Act did not create a substantive change, but rather "simply clarified existing U.S. law on this issue; it did not change the existing high standards under the U.S. law that must be met before law enforcement agencies can require disclosure of electronic data."[350] Nonetheless, privacy rights groups remain skeptical of the Act,[351] and Gibson Dunn will continue to monitor developments in this area.

2. Foreign Intelligence Surveillance Court Approves FBI's Proposed Electronic Surveillance Procedures

This fall, the Foreign Intelligence Security Court ("FISC") considered whether the FBI's protocols for identifying targets for electronic surveillance and collecting their data complied with the Foreign Intelligence Surveillance Act ("FISA") and with the Fourth Amendment.[352] On September 4, FISC upheld the certifications, approving a procedure under which: (1) the FBI differentiates between queries of U.S. persons and all other queries; (2) prior to reviewing the contents of any U.S. person query, the FBI provides a written statement as to why such query is reasonably likely to return foreign intelligence information or evidence of a crime; and (3) the FBI provides records of such queries to the Department of Justice and the Office of the Director of National Intelligence for oversight.[353] Additionally, the FISC affirmed that the NSA's 2018 Targeting Procedures prohibit collection of communications solely containing reference to, but not to or from, a foreign intelligence target (also known as "abouts" collection).[354]

3. Increased Government Use of Biometric Identification Technologies Draws Scrutiny

On October 31, 2019, the American Civil Liberties Union ("ACLU") filed a complaint against the FBI, DOJ and the Drug Enforcement Administration to compel the release of its policies, contracts and other records relating to the use of facial recognition programs and other biometric identification and tracking technology. The complaint argues that such "highly invasive" technologies permit the U.S. government to track people and their

associations in potentially unconstitutional ways.[355] For example, according to an FBI witness, the FBI has the ability to run facial recognition searches against over 640 million photographs.[356] The FBI's guidelines permit the use of such technology without a warrant, demonstration of probable cause, or other fact-based suspicion.[357]

Similarly, Immigration and Customs Enforcement ("ICE") has recently been scrutinized for its use of "Rapid DNA" testing on families at the U.S.-Mexico border to identify biological parent-child relationships within 90 minutes.[358] The Electronic Frontier Foundation filed suit this fall seeking records of ICE's testing procedures and accuracy, arguing that Rapid DNA testing is error-prone and expressing concern over the technology's use on lawful residents in non-border circumstances.[359]

Also in light of concerns regarding invasiveness and accuracy, three municipalities in California and one in Massachusetts have banned the municipal government from using facial recognition systems altogether.[360] At the state level, California and Massachusetts are considering laws to place a moratorium on government use of facial recognition and other biometric identification technologies until regulations are established to protect the public's interest.[361] At the federal level, the U.S. Congress has held multiple hearings throughout 2019 on the government's use of facial recognition, and several bills have been introduced to prohibit and/or limit such use.[362]

IV. Conclusion

2019 has proven to be another significant year in the development and application of data privacy and cybersecurity law and for 2020 the fast pace of change will continue. As technology and data collection become more sophisticated, companies, governments and the public at large will continue to explore the opportunities, and perils, that these changes present. We will be tracking these important issues in the year ahead.

---

[1] Eric Goldman, *What we've learned from California's Consumer Privacy Act so far*, The Hill (Jan. 11, 2020), *available at* https://thehill.com/opinion/cybersecurity/477821-what-weve-learned-from-the-california-consumer-privacy-act-so-far.

[2] *See, e.g., California Consumer Privacy Act: Compliance Heading into the New Year*, Gibson Dunn (Dec. 12, 2019), *available at* https://www.gibsondunn.com/california-consumer-privacy-act-compliance-heading-into-the-new-year/; *California Consumer Privacy Act Final Amendments Signed*, Gibson Dunn (Oct. 16, 2019), *available at* https://www.gibsondunn.com/california-consumer-privacy-act-2019-final-amendments-signed/; *California Consumer Privacy Act Update: Regulatory Update*, Gibson Dunn (Oct. 11, 2019), *available at* https://www.gibsondunn.com/california-consumer-privacy-act-update-regulatory-update/; *California Consumer Privacy Act Update — California State Committees Vote on Amendments*, Gibson Dunn (Apr. 30, 2019), *available at* https://www.gibsondunn.com/california-consumer-privacy-act-update-california-state-committees-vote-on-amendments/.

[3] California SB-1121 requires that the final regulations be published on or before July 1, 2020.

[4] Laura Mahoney, *California Governor Signs Bills to Refine Sweeping Privacy Law*, Bloomberg Law (Oct. 12, 2019), *available at* https://news.bloomberglaw.com/privacy-and-data-security/california-governor-signs-bills-to-refine-sweeping-privacy-law.

[5] Allison Grande, *Calif. Voters May Get Chance To Tighten Privacy Law,* Law360

(Sept. 25, 2019), *available at* https://www.law360.com/articles/1202779/calif-voters-may-get-chance-to-tighten-privacy-law.

[6] Cal. Civ. Code §§ 1798.100, 1798.140.

[7] *Id.*

[8] Mark Anderson, *California privacy law to take effect immediately in 2020, AG says,* Sacramento Business Journal (last updated Dec. 17, 2019), *available at* https://www.bizjournals.com/sacramento/news/2019/12/16/california-to-start-enforcing-privacy-law.html.

[9] Alexei Koseff, *California promises aggressive enforcement of new privacy law*, S.F. Chronicle (Dec. 16, 2019), *available at* https://www.sfchronicle.com/politics/article/California-promises-aggressive-enforcement-of-new-14911017.php.

[10] *Id.*

[11] Cal. Civ. Code §§ 1798.100, 1798.150.

[12] Act relating to Internet privacy, S.B. 220 (Nev. 2019), *available at* https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Text.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] Act to Protect the Privacy of Online Customer Information, S. P. 275 (Me. 2019), *available at* http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=1&snum=129.

[18] *Id.*

[19] *Id.*

[20] Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), S5575B (N.Y. 2019), *available at* https://www.nysenate.gov/legislation/bills/2019/s5575.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] An to amend the general business law, in relation to the management and oversight of personal data (New York Privacy Act), S.5842 (N.Y. 2019), *available at* https://legislation.nysenate.gov/pdf/bills/2019/S5642/.

[26] Lucas Ropek, *NY's Data Privacy Bill Failed; Is There Hope Next Session?*, Government Technology (July 15, 2019), *available at* https://www.govtech.com/policy/NYs-Data-Privacy-Bill-Failed-Is-There-Hope-Next-Session.html.

[27] Allison Schiff, *State Legislatures Are Back In Session, So Expect New Privacy*

Bills. Next Up: Washington State, AdExchanger (Jan. 14, 2020), *available at* https://adexchanger.com/privacy/state-legislatures-are-back-in-session-so-expect-new-privacy-bills-next-up-washington-state/.

[28] Act Relating to the management and oversight of personal data, S.B. 5376 (Wash. 2019), *available at* https://app.leg.wa.gov/billsummary?BillNumber=5376&Year=2019&Initiative=false.

[29] *Id.*

[30] Act to amend the general business law, in relation to the management and oversight of personal data, S.5642 (N.Y. 2019), *available at* https://www.nysenate.gov/legislation/bills/2019/s5642.

[31] *Id.*

[32] *Id.*

[33] *See, e.g.,* Allison Schiff, *State Legislatures Are Back In Session, So Expect New Privacy Bills. Next Up: Washington State*, AdExchanger (Jan. 14, 2020), *available at* https://adexchanger.com/privacy/state-legislatures-are-back-in-session-so-expect-new-privacy-bills-next-up-washington-state/.

[34] Senate Democrat Privacy Principles, Senate Democrats (Nov. 14, 2019), *available at* https://www.democrats.senate.gov/imo/media/doc/Final_CMTE%20Privacy%20Principles_11.14.19.pdf.

[35] *See, e.g.*, Lauren Feiner, *A federal privacy law is starting to crystallize, but Democrats and Republicans can't agree on how to do it*, CNBC (last updated Dec. 4, 2019), *available at* https://www.cnbc.com/2019/12/04/a-federal-privacy-law-is-starting-to-crystallize-senators-remain-divided-over-details.html.

[36] *See, e.g.*, Abbie Gruwell, *Preemption Takes Center Stage Amid Federal Data Privacy Action,* The National Conference of State Legislatures Blog (Apr. 8, 2019), *available at* https://www.ncsl.org/blog/2019/04/08/preemption-takes-center-stage-amid-federal-data-privacy-action.aspx.

[37] *See, e.g.*, Cameron F. Kerry, *Will this new Congress be the one to pass data privacy legislation?*, Brookings (Jan. 7, 2019), *available at* https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/.

[38] House Energy and Commerce Committee Staff Bipartisan Draft Privacy Bill (2019), *available at* https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/2019.12.18-Privacy-Bipartsian-Staff-Discussion-Draft.pdf.

[39] Emily Birnbaum, *Key House committee offers online privacy bill draft*, The Hill (Dec. 18, 2019), *available at* https://thehill.com/policy/technology/475191-key-house-committee-offers-online-privacy-bill-draft.

[40] House Energy and Commerce Committee Staff Bipartisan Draft Privacy Bill (2019), *available at* https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/2019.12.18-Privacy-Bipartsian-Staff-Discussion-Draft.pdf.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] S. 2968, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/2968?q=%7B%22search%22%3A%5B%22cantwell%22%5D%7D&s=3&r=3.

[46] United States Consumer Data Privacy Act of 2019 Staff Discussion Draft (2019), *available at* https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf.

[47] *Id.*

[48] *Id*; S. 2968, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/2968?q=%7B%22search%22%3A%5B%22cantwell%22%5D%7D&s=3&r=3.

[49] H.R. 4978, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/4978/text.

[50] S. 1951, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1951/text.

[51] S. 1578, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1578/text.

[52] S. 189, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/189/text.

[53] H.R. 2231, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/2231/text.

[54] S. 1116. 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1116/text.

[55] S. 1214, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1214/text.

[56] H.R. 2013, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/2013/text.

[57] S. 583, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/583/text.

[58] H.R. 5573, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/5573/text.

[59] S. 1578, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1578/text.

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] H.R. 2231, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/2231/text.

[64] *Id.*

[65] H.R. 5573, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/5573/text.

[66] S. 748, 116th Cong (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/748/text.

[67] H.R. 5573, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/5573/text; S. 748, 116th Cong (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/748/text.

[68] H.R. 5573, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/5573/text.

[69] S. 748, 116th Cong (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/748/text.

[70] *See* Prepared Opening Remarks of Chairman Joseph Simons, *Hearings on Competition and Consumer Protection in the 21st Century*, The FTC's Approach to Consumer Privacy (Apr. 9, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1512673/chmn-simons-opening_remarks_ftc_hearing_12.pdf; Remarks of Chairman Joseph Simons, *Hearings on Competition and Consumer Protection in the 21st Century*, *Session on FTC's Role in a Changing World* (Mar. 25, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1508536/oia_hearing_march_25_remarks_chmn_simons.pdf.

[71] Press Release, Federal Trade Commission, *FTC Seeks to Examine the Privacy Practices of Broadband Providers* (Mar. 26, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers.

[72] *See, e.g.*, Andrew Smith, *New and improved FTC data security orders: Better guidance for companies, better protection for consumers*, Federal Trade Commission Blog (Jan. 6, 2020), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance.

[73] *See, e.g.,* Remarks of Commissioner Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law* (Sept. 6, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf.

[74] *See* Remarks of Commissioner Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law* (Sept. 6, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf; Prepared Remarks of Chairman Joseph Simons, *Introductory Keynote: American Bar Association Consumer Protection Conference* (Feb. 5, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1451379/simons-_nashville-aba-remarks.pdf.

[75] *See* Prepared Remarks of Chairman Joseph Simons, *Introductory Keynote: American Bar Association Consumer Protection Conference* (Feb. 5, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1451379/simons-_nashville-aba-remarks.pdf.

[76] Press Release, Federal Trade Commission, *FTC Grants Final Approval to Settlement with Former Cambridge Analytica CEO, App Developer over Allegations they Deceived Consumers over Collection of Facebook Data* (Dec. 18, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/12/ftc-grants-final-approval-settlement-former-cambridge-analytica.

[77] *Id.*

[78] *Id.*

[79] *See, e.g.*, Press Release, United Kingdom Information Commissioner's Office, *SCL Elections prosecuted for failing to comply with enforcement notice* (Jan. 9, 2019), *available at* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/01/scl-elections-prosecuted-for-failing-to-comply-with-enforcement-notice/.

[80] Press Release, Federal Trade Commission, *FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield* (Dec. 6, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving.

[81] *Id.*

[82] *Id.*

[83] Press Release, Federal Trade Commission, *FTC Finalizes Settlement with Company that Misled Consumers about how it Accesses and Uses their Email* (Dec. 17, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/12/ftc-finalizes-settlement-company-misled-consumers-about-how-it.

[84] *Id.*

[85] *Id.*

[86] *Id.*

[87] Press Release, Federal Trade Commission, *Utah Company Settles FTC Allegations it Failed to Safeguard Consumer Data* (Nov. 12, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/11/utah-company-settles-ftc-allegations-it-failed-safeguard-consumer.

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] Press Release, Federal Trade Commission, *FTC Brings First Case Against Developers of "Stalking" Apps* (Oct. 22, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps; *see also FTC Brings First Case Against Tracking Apps*, Gibson Dunn (Nov. 1, 2019), *available at* https://www.gibsondunn.com/california-consumer-privacy-act-2019-final-amendments-signed/.

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] Press Release, Federal Trade Commission, *FTC Gives Final Approval to Settlement with Auto Dealer Software Company That Allegedly Failed to Protect Consumers' Data* (Sept. 6, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/09/ftc-gives-final-approval-settlement-auto-dealer-software-company.

[99] *Id.*

[100] *Federal Trade Commission* (F.T.C.), *In re LightYear Dealer Technologies, LLC*, Docket No. C-4687 (F.T.C. Sept. 6, 2019), *available at* https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf.

[101] *Id.*

[102] Press Release, Federal Trade Commission, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law* (Sept. 4, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] Press Release, Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[109] *Id.*

[110] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *United States v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C. July 24, 2019), ECF No. 2-1, *available at* https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] Press Release, Federal Trade Commission, *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* (July 22, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] Press Release, Federal Trade Commission, *D-Link Agrees to Make Security Enhancements to Settle FTC Litigation* (July 2, 2019), *available at* https://www.ftc.gov/new

s-events/press-releases/2019/07/d-link-agrees-make-security-enhancements-settle-ftc-litigation.

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] Press Release, Federal Trade Commission, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law* (Feb. 27, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] Press Release, Federal Trade Commission, *FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield* (Dec. 6, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving; Press Release, Federal Trade Commission, *California Company Settles FTC Allegations that it Falsely Claimed Participation in EU-U.S. Privacy Shield* (Nov. 19, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/11/california-company-settles-ftc-allegations-it-falsely-claimed; Press Release, Federal Trade Commission, *FTC Charges Nevada Company with Falsely Claiming Participation in the EU-U.S. Privacy Shield* (Nov. 7, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/11/ftc-charges-nevada-company-falsely-claiming-participation-eu-us; Press Release, Federal Trade Commission, *FTC Approves Final Consent Order Settling Charges That Background Screening Company Falsely Claimed Compliance with EU-U.S. Privacy Shield Framework* (Aug. 21, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/08/ftc-approves-final-consent-order-settling-charges-background.

[127] *Id.*

[128] Press Release, Federal Trade Commission, *FTC Takes Action against Companies Falsely Claiming Compliance with the EU-U.S. Privacy Shield, Other International Privacy Agreements* (June 14, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/06/ftc-takes-action-against-companies-falsely-claiming-compliance-eu.

[129] Federal Trade Commission, *Privacy Shield*, *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield.

[130] *See* 15 U.S.C. § 53(b).

[131] *See FTC v. Commerce Planet, Inc.*, 815 F.3d 593, 598–99 (9th Cir. 2016); *FTC v. Ross*, 743 F.3d 886, 890–92 (4th Cir. 2014); *FTC v. Bronson Partners, LLC*, 654 F.3d 359, 365–66 (2d Cir. 2011); *FTC v. Magazine Sols., LLC*, 432 F. App'x 155, 158 n.2 (3d Cir. 2011) (unpublished); *FTC v. Direct Mktg. Concepts, Inc.*, 624 F.3d 1, 15 (1st Cir. 2010); *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202 n.6 (10th Cir. 2005); *FTC v. Gem Merch. Corp.*, 87 F.3d 466, 468–70 (11th Cir. 1996); *FTC v. Security Rare Coin & Bullion Corp.*, 931 F.2d 1312, 1314–15 (8th Cir. 1991); *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 571–72 (7th Cir. 1989).

[132] *FTC v. Credit Bureau Ctr., LLC*, 937 F.3d 764 (7th Cir. 2019) (vacating a $5.26 million judgment in favor of the FTC).

[133] Petition for a Writ of Certiorari, *FTC v. Credit Bureau Ctr., LLC*, No. 19-____ (U.S. Dec. 19, 2019), available at https://www.ftc.gov/system/files/documents/cases/petitionforawritofcertiorari_no._19.pdf.

[134] *See, e.g.*, Remarks of Commissioner Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law* (Sept. 6, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf; Prepared Remarks of Chairman Joseph Simons, *Introductory Keynote: American Bar Association Consumer Protection Conference* (Feb. 5, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1451379/simons-_nashville-aba-remarks.pdf.

[135] Press Release, Department of Health and Human Services, *OCR Concludes All-Time Record Year for HIPAA Enforcement with $3 Million Cottage Health Settlement* (Feb. 7, 2019), *available at* https://www.hhs.gov/about/news/2019/02/07/ocr-concludes-all-time-record-year-for-hipaa-enforcement-with-3-million-cottage-health-settlement.html.

[136] Ben Kochman, *HIPAA Enforcers Lower Fines For Less Serious Violations*, Law360 (Apr. 26, 2019), *available at* https://www.law360.com/articles/1154042/hipaa-enforcers-lower-fines-for-less-serious-violations.

[137] *See, e.g.*, Dena Castricone, *HIPAA Compliance Lessons From 2019 Enforcement Trends*, Law360 (Jan. 22, 2020), *available at* https://www.law360.com/articles/1236238/hipaa-compliance-lessons-from-2019-enforcement-trends.

[138] Press Release, Department of Health and Human Services, *Tennessee Diagnostic Medical Imaging Services Company Pays $3,000,000 to Settle Breach Exposing over 300,000 Patients' Protected Health Information* (May 6, 2019), *available at* https://www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html.

[139] *Id.*

[140] Press Release, Department of Health and Human Services, *OCR Imposes a $1.6 Million Civil Money Penalty against Texas Health and Human Services Commission for HIPAA Violations* (Nov. 7, 2019), *available at* https://www.hhs.gov/about/news/2019/11/07/ocr-imposes-a-1.6-million-dollar-civil-money-penalty-against-tx-hhsc-for-hipaa-violations.html.

[141] Press Release, Department of Health and Human Services, *Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement* (Nov. 5, 2019), *available at* https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html.

[142] *Id.*

[143] Press Release, Department of Health and Human Services, *OCR Settles First Case in HIPAA Right of Access Initiative* (Sept. 9, 2019), *available at* https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html.

[144] *Id.*

[145] Press Release, Department of Health and Human Services, *OCR Settles Second Case in HIPAA Right of Access Initiative* (Dec. 12, 2019), *available at* https://www.hhs.gov/about/news/2019/12/12/ocr-settles-second-case-in-hipaa-right-of-access-initiative.html.

[146] Press Release, Department of Health and Human Services, *OCR Settles First Case in HIPAA Right of Access Initiative* (Sept. 9, 2019), *available at* https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html; Press Release, Department of Health and Human Services, *OCR Settles Second Case in HIPAA Right of Access Initiative* (Dec. 12, 2019), *available at* https://www.hhs.gov/about/news/2019/12/12/ocr-settles-second-case-in-hipaa-right-of-access-initiative.html.

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

[148] *See* Complaint, *Univ. of Tex. MD Anderson Cancer Ctr. v. Azar*, Docket No. 4:19-cv-01298 (S.D. Tex. Apr. 9, 2019), ECF No. 1.

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

[150] *See* Request for Information on Modifying HIPAA Rules to Improve Coordinated Care, regulations.gov, *available at* https://www.regulations.gov/docket?D=HHS-OCR-2018-0028.

[151] *See, e.g.*, Comment of Wash. State Dep't of Soc. and Health Servs., Request for Information on Modifying HIPAA Rules To Improve Coordinated Care, FR Docket No. 2018-27162 (Feb. 12, 2019), *available at* https://www.regulations.gov/document?D=HHS-OCR-2018-0028-1095.

[152] *See, e.g.*, Comment of Nat'l Disability Rights Network, Request for Information on Modifying HIPAA Rules To Improve Coordinated Care, FR Docket No. 2018-27162 (Feb. 12, 2019), *available at* https://www.regulations.gov/document?D=HHS-OCR-2018-0028-1294.

[153] *See, e.g.*, Comment of Nat'l Ass'n of Chain Drug Stores, Request for Information on Modifying HIPAA Rules To Improve Coordinated Care, FR Docket No. 2018-27162 (Feb. 11, 2019), *available at* https://www.regulations.gov/document?D=HHS-OCR-2018-0028-0874.

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

[155] *Id.*

[156] Consent Judgment and Order, *State of Arizona v. Med. Informatics Eng'g, Inc.*, No. 3:18-cv-00969 (N.D. Ind. May 28, 2019), ECF No. 66.

[157] SEC Office of Compliance Inspection and Examinations, *Risk Alert - Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies* (Apr. 16, 2019), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf.

[158] *Id.* at 2–3.

[159] *Id.* at 3–4.

[160] Press Release, *SEC Office of Compliance Inspections and Examinations Announces 2020 Examination Priorities* (Jan. 7, 2020), *available*

at https://www.sec.gov/news/press-release/2020-4.

[161] *Id.*

[162] *Id.*

[163] U.S. Securities and Exchange Commission, *Electronic Data Gathering, Analysis, and Retrieval*, *available at* https://www.sec.gov/edgar.shtml (last visited Jan. 23, 2020).

[164] Complaint, *SEC v. Ieremenko et al.*, No. 2:19-cv-00505 (D.N.J. Jan. 15, 2019), ECF No. 1.

[165] Press Release, U.S. Securities and Exchange Commission, *SEC Brings Charges in EDGAR Hacking Case* (Jan. 15, 2019), *available at* https://www.sec.gov/news/press-release/2019-1.

[166] Press Release, U.S. Securities and Exchange Commission, *Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data* (July 24, 2019), *available at* https://www.sec.gov/news/press-release/2019-140.

[167] Press Release, U.S. Securities and Exchange Commission, *SEC and CFTC Charge Options Clearing Corp. with Failing to Establish and Maintain Adequate Risk Management Policies* (Sept. 4, 2019), *available at* https://www.sec.gov/news/press-release/2019-171.

[168] SEC Division of Enforcement, *2019 Annual Report* at 13, *available at* https://www.sec.gov/files/enforcement-annual-report-2019.pdf.

[169] Press Release, U.S. Securities and Exchange Commission, *Company Settles Unregistered ICO Charges After Self-Reporting to SEC* (Feb. 20, 2019), *available at* https://www.sec.gov/news/press-release/2019-15.

[170] Complaint, *SEC v. Telegram Group Inc. et al.*, No. 1:19-cv-9439 (S.D.N.Y. Oct. 11, 2019), ECF No. 1; *see also* Press Release, U.S. Securities and Exchange Commission, *SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering* (Oct. 11, 2019), *available at* https://www.sec.gov/news/press-release/2019-212.

[171] Complaint, *SEC v. Eyal*, No. 1:19-cv-11325 (S.D.N.Y. Dec. 11, 2019), ECF No. 1.

[172] TurnKey Jet, Inc., SEC No-Action Letter (Apr. 3, 2019), *available at* https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

[173] *Id*.

[174] *See* Advanced Methods to Target and Eliminate Unlawful Robocalls, *Declaratory Ruling and Third Further Notice of Proposed Rulemaking*, FCC 19-51, 34 FCC Rcd. 4876 (June 6, 2019).

[175] In the Matters of Implementing Section 503 of RAY BAUM'S Act, *Second Report and Order*, FCC Rcd. 19-73 (Aug. 1, 2019), *available at* https://docs.fcc.gov/public/attachments/FCC-19-73A1.pdf

[176] STIR/SHAKEN stands for "Secure Telephony Identity Revisited/ Secure Handling of Asserted information using toKEN."

[177] Ajit Pai, Comm'r, FCC, *Remarks at the Robocall Symposium of New England States* (Nov. 21, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-360946A1.pdf

[178] Press Release, FCC, *Chairman Pai Statement on Progress by Major Phone Companies in Implementing Caller ID Authentication* (Aug. 14, 2019), *available at* https://docs.fcc.gov/public/attachments/DOC-359087A1.pdf.

[179] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019).

[180] *Id.*

[181] *See, e.g.*, Cassell Bryan-Low et al., *Special report - Hobbling Huawei: Inside the U.S. war on China's tech giant*, Reuters (May 21, 2019), *available at* https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSKCN1SR1EU; Diane Bartz & Christian Shepherd, *U.S. legislation steps up pressure on Huawei and ZTE, China calls it 'hysteria'*, Reuters (Jan. 16, 2019), *available at* https://www.reuters.com/article/us-usa-china-huawei-tech/u-s-legislation-steps-up-pressure-on-huawei-and-zte-china-calls-it-hysteria-idUSKCN1PA2LU.

[182] *In the Matter of Protecting Against Nat'l Security Threats to the Comm'ns Supply Chain Through FCC Programs*, *Report and Order, Further Notice of Proposed Rulemaking, and Order*, FCC 19-121 (Nov. 22, 2019), *available at* https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

[183] *See* Petition for Review, *Huawei Techs. v. FCC*, No. 19-60896 (5th Cir. Dec. 5, 2019), *available at* https://prodnet.www.neca.org/publicationsdocs/wwpdf/12519huawei.pdf; *see also* Petition for Review, *Huawei Technologies USA, Inc. et al. v. Federal Communications Commission et al.*, No 19-60896 (5th Cir. Jan. 7, 2020).

[184] *In the Matter of Protecting Against Nat'l Security Threats to the Comm'ns Supply Chain Through FCC Programs*, *Report and Order, Further Notice of Proposed Rulemaking, and Order*, FCC 19–121, ¶¶ 122-60 (Nov. 22, 2019), *available at* https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

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

[186] *Id.*

[187] Brief for the Respondent, *Seila Law LLC v. CFPB*, No. 19-7 (U.S. Sept. 17, 2019).

[188] *Seila Law LLC v. CFPB*, 140 S. Ct. 427 (2019) (granting certiorari). *Barr v. Am. Ass'n of Political Consultants Inc.*,

[189] Press Release, CFPB, *CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach* (July 22, 2019), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/.

[190] *Id.*

[191] Dep't of Defense, Defense Contract Mgmt. Agency, *Contractor Purchasing System Review (CPSR) Guidebook* (June 14, 2019), *available at* https://www.dcma.mil/Portals/31/Documents/CPSR/CPSR_Guidebook_062719.pdf

[192] *Id.* at 97.

[193] *See, e.g.*, *id.* at 103–05.

[194] U.S. Dep't of Defense Office of the Under Secretary of Defense for Acquisition & Sustainment, *Cybersecurity Maturity Model Certification (CMMC) Version 0.7* (Dec. 6, 2019), *available at* https://www.acq.osd.mil/cmmc/docs/CMMC_Version0.7_UpdatedCompiledDeliverable_20191209.pdf.

[195] U.S. Dep't of Defense Office of the Under Secretary of Defense for Acquisition & Sustainment, *Welcome Page*, *available at* https://www.acq.osd.mil/cmmc/index.html.

[196] U.S. Dep't of Defense Office of the Under Secretary of Defense for Acquisition & Sustainment, *Cybersecurity Maturity Model Certification (CMMC) Version 0.7* (Dec. 6, 2019), *available at* https://www.acq.osd.mil/cmmc/docs/CMMC_Version0.7_UpdatedCompiledDeliverable_20191209.pdf.

[197] Travis J. Tritten, *Defense Contractors to Face Added Costs With Cybersecurity Audit*, Bloomberg Gov't (Jan. 15, 2020), *available at* https://about.bgov.com/news/defense-contractors-to-face-added-costs-with-cybersecurity-audit/.

[198] U.S. Dep't of Defense Inspector General, *Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items* (July 26, 2019), *available at* https://media.defense.gov/2019/Jul/30/2002164272/-1/-1/1/DODIG-2019-106.PDF.

[199] U.S. Dep't of Defense Inspector General, *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems* (July 23, 2019), *available at* https://media.defense.gov/2019/Jul/25/2002162331/-1/-1/1/DODIG-2019-105.PDF.

[200] National Defense Authorization Act (NDAA) for Fiscal Year 2020, Pub. L. No. 116-92, 133 Stat 1198 (2019).

[201] *Id.*

[202] Press Release, DOJ, *Justice Department Reviewing the Practices of Market-Leading Online Platforms* (July 23, 2019), *available at* https://www.justice.gov/opa/pr/justice-department-reviewing-practices-market-leading-online-platforms.

[203] Tony Romm, *DOJ issues new warning to big tech: Data and privacy could be competition concerns*, Wash. Post (Nov. 8, 2019), *available at* https://www.washingtonpost.com/technology/2019/11/08/doj-issues-latest-warning-big-tech-data-privacy-could-be-competition-concerns/.

[204] Press Release, CFTC, *CFTC Orders Registrant to Pay $1.5 Million for Violations Related to Cyber Breach* (Sept. 12, 2019), *available at* https://www.cftc.gov/PressRoom/PressReleases/8008-19.

[205] Press Release, Dep't of Commerce, *U.S. Department of Commerce Proposes Rule for Securing the Nation's Information and Communications Technology and Services Supply Chain* (Nov. 26, 2019), *available at* https://www.commerce.gov/news/press-releases/2019/11/us-department-commerce-proposes-rule-securing-nations-information-and.

[206] Brandi Vincent, *How the Energy Department Is Prioritizing Secure Infrastructure*, Nextgov (Mar. 21, 2019), *available at* https://www.nextgov.com/cybersecurity/2019/03/how-energy-department-prioritizing-secure-infrastructure/155734/.

[207] *See, e.g.*, GAO-19-332, *Critical Infrastructure Protection, Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid* (Aug. 2019), *available at* https://www.gao.gov/assets/710/701079.pdf.

[208] DHS Office of Inspector General, *Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information (REDACTED)* (Mar. 15, 2019), *available at* https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-32-Mar19.pdf.

[209] Nat'l Institute of Standards and Tech., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (June 2019), *available at* https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/draft.

[210] *Id.* at iv.

[211] Nat'l Institute of Standards and Tech., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets* (June 2019), *available at* https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-draft-ipd.pdf.

[212] *Id.* at iv (emphases omitted).

[213] Nat'l Institute of Standards and Tech., *NIST Releases Version 1.0 of Privacy Framework* (Jan. 16, 2020), *available at* https://www.nist.gov/news-events/news/2020/01/nist-releases-version-10-privacy-framework.

[214] Final Judgment and Consent Decree, *The State of Alabama v. Equifax, Inc.* (July 19, 2019), *available at* https://www.sec.gov/Archives/edgar/data/33185/000119312519198584/d734596dex104.htm.

[215] *See* Press Release, NY State Office of the Attorney General, *Attorney General James Secures $6 Million From Cisco Systems In Multistate Settlement* (Aug. 1, 2019), *available at* https://ag.ny.gov/press-release/2019/attorney-general-james-secures-6-million-cisco-systems-multistate-settlement; Mark Chandler, *Executive Platform: A Changed Environment Requires a Changed Approach*, Cisco Blogs (July 31, 2019), *available at* https://blogs.cisco.com/news/a-changed-environment-requires-a-changed-approach.

[216] Press Release, N.Y. Dep't Fin. Serv., *Attorney General James Gives Update on Facebook Antitrust Investigation* (Oct. 22, 2019), *available at* https://ag.ny.gov/press-release/2019/attorney-general-james-gives-update-facebook-antitrust-investigation.

[217] Press Release, Office of the Attorney Gen., *NJ Announces New "Cyber Savvy Youth" Initiative to Keep Kids Safe Online and Releases Annual Statistics on Cyber Breaches* (Oct. 31, 2019), *available at* https://www.nj.gov/oag/newsreleases19/pr20191031a.html.

[218] Press Release, N.Y. Dep't Fin. Serv., *Acting Superintendent Linda A. Lacewell Names Justin Herring Executive Deputy Superintendent of Newly Created Cybersecurity Division* (May 22, 2019), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1905221.

[219] *See* RiskBased Security, *Data Breach Quickview Report, 2019 Q3 Trends* (Nov. 2019), *available at* https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf.

[220] Christopher Rowland, *Quest Diagnostics Discloses Breach of Patient Records*, Wash. Post (June 3, 2019), *available at* https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html.

[221] Jessica Davis, *Quest, Labcorp, AMCA Face Breach Lawsuits, State Investigations*, Health Security (June 11, 2019), *available at* https://healthitsecurity.com/news/quest-labcorp-amca-face-hit-by-breach-lawsuits-state-investigations.

[222] *Id.*

[223] Ben Kochman, *Debt Collection Co. Files Ch. 11 After Health Data Breach* (June 11, 2019), *available at* https://www.law360.com/articles/1170470?scroll=1&related=1.

[224] Taylor Telford, *Wawa Hit With Massive Data Breach, Potentially Affecting More Than 850 Locations, CEO Says*, Wash. Post (Dec. 20, 2019), *available at* https://www.washingtonpost.com/business/2019/12/20/wawa-hit-with-massive-data-breach-potentially-affecting-all-locations-ceo-says/.

[225] Matt Fair, *Firm Says Lead Counsel Bids in Wawa Suits Should Wait*, Law360 (Jan. 3, 2020), *available at* https://www.law360.com/articles/1231110/firm-says-lead-counsel-bids-in-wawa-suits-should-wait.

[226] Allison Grande, *Contested Equifax Data Breach Deal Gets Final Nod*, Law360 (Dec. 20, 2019), *available at* https://www.law360.com/articles/1230211/contested-equifax-data-breach-deal-gets-final-nod.

[227] *Id.*; *see also* Allison Grande, *Equifax Data Breach Settlement Is A Good Deal, Judge Says*, Law360 (Jan. 15, 2020), *available at* https://www.law360.com/articles/1234404?scroll=1&related=1.

[228] Allison Grande, *Equifax Data Breach Settlement Is A Good Deal, Judge Says*, Law360 (Jan. 15, 2020), *available at* https://www.law360.com/articles/1234404?scroll=1&related=1.

[229] Order Granting Preliminary Approval, *In Re: Yahoo! Inc. Customer Data Security Breach Litigation*, 5:16-MD-02752 (N.D. Cal. July 20, 2019), ECF No. 390.

[230] *Id.*

[231] Dorothy Atkins, *Yahoo's Revised $117M Data Breach Deal Gets Koh's Initial OK*, Law360 (July 22, 2019), *available at* https://www.law360.com/articles/1180718/yahoo-s-revised-117m-data-breach-deal-gets-koh-s-initial-ok.

[232] Vince Sullivan, *$29M Yahoo Breach Deal in Calif. Ends Chancery Suit in Del.*, Law360 (Jan. 11, 2019), *available at* https://www.law360.com/articles/1117984/-29m-yahoo-breach-deal-in-calif-ends-chancery-suit-in-del-.

[233] Order Granting in Part and Denying in Part Facebook Inc.'s Motion to Dismiss, *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, No. 18-MD-02843 (N.D. Cal. Sept. 9, 2019), ECF No. 298.

[234] *Id.*

[235] Pretrial Order No. 26: Order Denying Motion to Certify for Interlocutory Appeal, *In re: Facebook, Inc. Consumer Privacy User Profile Litig.*, No. 18-MD02843-VC (N.D. Cal. Oct. 31, 2019), ECF No. 330.

[236] Pretrial Order No. 32: Case Management Schedule, *In re: Facebook, Inc. Consumer Privacy User Profile Litig.*, No. 18-MD02843-VC (N.D. Cal. Dec. 13, 2019), ECF

No. 356.

[237] Hamza Shaban, *Under Armour Announces Data Breach, Affecting 150 million MyFitnessPal App Accounts*, Wash. Post (Mar. 29, 2018), *available at* https://www.washingtonpost.com/news/theswitch/wp/2018/03/29/under-armour-announces-data-breach-affecting-150-million-myfitnesspal-appaccounts.

[238] Order, *Murray v. Under Armour, Inc.*, 18-cv-04032 (C.D. Cal. Feb. 11, 2019), ECF No. 36.

[239] 136 S. Ct. 1540 (2016).

[240] *Id.* at 1549.

[241] *See, e.g.*, *In re Zappos.com, Inc.*, 888 F.3d 1020, 1028 (9th Cir. 2018); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017).

[242] *See, e.g.*, *Beck v. McDonald*, 848 F.3d 262, 266-67 (4th Cir. 2017); *In re SuperValu, Inc.*, 870 F.3d 763, 771–72 (8th Cir. 2017).

[243] *In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 61 (D.C. Cir. 2019) (quoting *Attias v. Carefirst, Inc.*, 865 F.3d 620, 622 (D.C. Cir. 2017)).

[244] 865 F.3d 620, 628 (D.C. Cir. 2017).

[245] *In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 58 (D.C. Cir. 2019) .

[246] *Id.* at 59.

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

[248] *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018). *See Zappos.com, Inc. v. Stevens*, No. 18-225, Doc. No. 13 (Mar. 25, 2019) (denying certiorari).

[249] *Consumer and Governmental Affairs Bureau Seeks Comment on Petition For Expedited Declaratory Ruling Filed By SGS North America, Inc.*, GC Docket No. 02-278 (Dec. 20, 2018), *available at* https://ecfsapi.fcc.gov/file/12212239203475/DA-18-1290A1.pdf (noting comment period closes in February of 2020).

[250] *Petition For Expedited Declaratory Ruling or, in the Alternative, Request for Retroactive Waiver*, GC Docket No. 02-278 (Dec. 17, 2018), *available at* https://ecfsapi.fcc.gov/file/121726169703/SGS%20--%20FCC%20Petition%20for%20Declaratory%20Ruling.pdf.

[251] *Id.*

[252] *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, Federal Communications Commission, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51 (June 6, 2019), *available at* https://docs.fcc.gov/public/attachments/FCC-19-51A1.pdf

[253] *Id.* at 12–13.

[254] 139 S. Ct. 2051 (2019).

[255] *Id.*

[256] *Id.*

[257] *Id.* at 2056.

[258] *Id.* at 2058.

[259] *Id.*

[260] *Salcedo v. Hanna*, 936 F.3d 1162, 1172 (11th Cir. 2019).

[261] 847 F.3d 1037, 1043 (9th Cir. 2017).

[262] *Facebook, Inc. v. Duguid*, Petition for Writ of Certiorari, No. 19-511 (U.S. Oct. 17, 2019) ("Facebook Petition"); *Charter Commc'ns, Inc. v. Gallion*, Petition for Writ of Certiorari, No. 19-575 (U.S. Nov. 1, 2019).

[263] 904 F.3d 1041 (9th Cir. 2018).

[264] Facebook Petition at 23–29.

[265] 885 F.3d 687 (D.C. Cir. 2018). Gibson Dunn represented the U.S. Chamber of Commerce, one of the petitioners, in this case.

[266] *Barr v. Am Ass'n of Political Consultants Inc.*, No. 19-631 (U.S. Jan. 10, 2020) (granting certiorari).

[267] S. 151 116th Congress (2019-2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/151/text.

[268] *Id.*

[269] H.R. 3375 116th Congress (2019-2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/3375/text.

[270] 740 Ill. Comp. Stat. Ann. 14/20 (West 2008).

[271] 129 N.E.3d 1197 (Ill. 2019).

[272] *Id*. at 1206.

[273] 2019 WL 1049107 (Ill. App. Ct. Mar. 4, 2019).

[274] 409 F. Supp. 3d 612 (N.D. Ill. 2019).

[275] 2019 WL 6253807 (N.D. Ill. Nov. 22, 2019).

[276] *Id*. at *5.

[277] *Id*.

[278] 2019 WL 1560416 (Ill. App. Ct. Apr. 9, 2019).

[279] *Id*. at *4.

[280] *See generally* Plaintiff's Unopposed Motion and Memorandum in Support of Preliminary Approval of Class Action Settlement, *Dixon v. The Washington and Jane Smith Community-Beverly*, 2019 WL 2445292 (N.D. Ill. May 9, 2019) (No. 1:17-cv-08033).

[281] *See, e.g.*, Complaint, *Yozze v. Universal Parks & Resorts Mgmt. Servs. LLC*,

No. 2019-CH-06366 (Ill. Cir. Ct. May 23, 2019); Complaint*, Acaley v. Vimeo Inc.*, No. 2019-CH-10873 (Ill. Cir. Ct. Sept. 20, 2019); Complaint, *Miracle-Pond v. Shutterfly Inc.*, No. 2019-CH-07050 (Ill. Cir. Ct. June 11, 2019).

[282] *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019).

[283] *Id*. at 1267.

[284] *See* David Thacker, *Expediting changes to Google+*, Google (Dec. 10, 2018), *available at* https://www.blog.google/technology/safety-security/expediting-changes-google-plus/; *see also* Douglas MacMillan & Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, Wall Street Journal (Oct. 8, 2018), *available at* https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194; Lily Hay Newman, *A New Google+ Blunder Exposed Data from 52.5 Million Users*, Wired (Dec. 10, 2018), *available at* https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/.

[285] Joint Stipulation and [Proposed] Order re Plaintiffs' Filing of Amended Consolidated Complaint, *In re Google Plus Profile Litig.*, No. 5:18-cv-06164-EJD (N.D. Cal. Feb. 20, 2019), ECF No. 35.

[286] Joint Stipulation and [Proposed] Order to Continue Hearing Date for Motion for Preliminary Approval, *In re Google Plus Profile Litig.*, No. 5:18-cv-06164-EJD (VKD) (N.D. Cal. Dec. 5, 2019), ECF No. 55.

[287] Plaintiffs' Notice of Motion for Preliminary Approval of Class Action Settlement, Exhibit 1 (Settlement Agreement), *In re Google Plus Profile Litig.*, No. 5:18-cv-06164-EJD (VKD) (N.D. Cal. Jan. 6, 2020), ECF No. 57-2.

[288] Defendants' Notice of Motion and Motion to Dismiss Consolidated Amended Complaint for Violation of the Federal Securities Laws and Memorandum of Points and Authorities in Support at 2, *In re Alphabet, Inc., Sec. Litig.*, No. 4:18-CV-06245-JSW (N.D. Cal. May 31, 2019), ECF No. 71.

[289] Order on Motions to Dismiss, Motion to Stay, and Motion to Intervene, *In re Facebook, Inc. S'holder Derivative Privacy Litig.*, No. 18-CV-01792-HSG (N.D. Cal. Mar. 22, 2019), ECF No. 113.

[290] *Id.* at 22.

[291] Plaintiffs' First Amended Consolidated Shareholder Derivative Complaint, *In re Facebook, Inc. S'holder Derivative Privacy Litig.*, No. 18-CV-01792-HSG (N.D. Cal. Dec. 17, 2019), ECF No. 142.

[292] Order Denying Defendant Facebook, Inc.'s Opposed Motion to Dismiss, or in the Alternative, to Stay Proceedings at 2, *District of Columbia v. Facebook*, No. 2018 CA 8715 B (D.C. Super. Ct. May 31, 2019).

[293] *Id.* at 24–29.

[294] Order Approving Stipulation of Dismissal, *Mulder v. Wells Fargo Bank, N.A.*, No. 2:18-CV-00029 (W.D. Pa. Feb. 5, 2019), ECF No. 58.

[295] *See Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427, 430–35 (Ct. App. 2018).

[296] Order Granting Defendant's Motion to Dismiss at 10, *In re: Google Location History Litig.*, No. 5:18-cv-05062-EJD (N.D. Cal. Dec. 19, 2019), ECF No. 113.

[297] *Id.* at 19.

[298] Defendant Google LLC's Motion to Dismiss Plaintiffs' Consolidated Complaint, *In re: Google Location History Litig.*, No. 5:18-cv-05062-EJD (N.D. Cal. May 28, 2019), ECF No. 87.

[299] Order Granting Defendant's Motion to Dismiss, *In re: Google Location History Litig.*, No. 5:18-cv-05062-EJD (N.D. Cal. Dec. 19, 2019), ECF No. 113.

[300] *Id.* at 2.

[301] *Id.*

[302] Complaint, *Dinerstein v. Google, LLC*, No. 19-cv-04311 (N.D. Ill. June 26, 2019), ECF No. 1; *see also* Amended Class Action Complaint and Demand for Jury Trial, *Dinerstein v. Google, LLC*, No. 19-cv-04311 (N.D. Ill. Oct. 8, 2019), ECF No. 42.

[303] Complaint at 2, *Dinerstein v. Google, LLC*, No. 19-cv-04311 (N.D. Ill. June 26, 2019), ECF No. 1.

[304] *Id.* at 17; Amended Class Action Complaint and Demand for Jury Trial at 2, *Dinerstein v. Google, LLC*, No. 19-cv-04311 (N.D. Ill. Oct. 8, 2019), ECF No. 42.

[305] Defendant Google LLC's Motion to Dismiss Plaintiff's Complaint, *Dinerstein v. Google, LLC*, No. 19-cv-04311 (N.D. Ill. Aug. 27, 2019), ECF No. 30; The University of Chicago and The University of Chicago Medical Center's Motion to Dismiss, *Dinerstein v. Google, LLC*, No. 19-cv-04311 (N.D. Ill. Aug. 27, 2019), ECF No. 26.

[306] *See* FCA US LLC's Motion to Decertify Classes, *Flynn v. FCA US LLC*, No. 3:15-CV-855-SMY-RJD (S.D. Ill. Nov. 11, 2019), ECF No. 550.

[307] United States Supreme Court Order List, United States Supreme Court, 18-398 (Jan. 7, 2019), *available at* https://www.supremecourt.gov/orders/courtorders/010719zor_m6ho.pdf.

[308] *See* FCA US LLC's Motion for Summary Judgment and Brief in Support of its Motion for Summary Judgment, *Flynn v. FCA US LLC*, No. 3:15-CV-855-SMY-RJD (S.D. Ill. Nov. 11, 2019), ECF Nos. 561, 562; FCA US LLC's Motion to Dismiss for Lack of Subject Matter Jurisdiction and Brief in Support of its Motion to Dismiss for Lack of Subject Matter Jurisdiction, *Flynn v. FCA US LLC*, No. 3:15-CV-855-SMY-RJD (S.D. Ill. Nov. 11, 2019), ECF Nos. 574, 575.

[309] *See* FCA US LLC's Brief in Support of its Motion for Summary Judgment at 1, *Flynn v. FCA US LLC*, No. 3:15-CV-855-SMY-RJD (S.D. Ill. Nov. 11, 2019), ECF No. 562; FCA US LLC's Brief in Support of its Motion to Dismiss for Lack of Subject Matter Jurisdiction, *Flynn v. FCA US LLC*, No. 3:15-CV-855-SMY-RJD (S.D. Ill. Nov. 11, 2019), ECF No. 575.

[310] *See* FCA US LLC's Brief in Support of its Motion to Dismiss for Lack of Subject Matter Jurisdiction at 12, *Flynn v. FCA US LLC*, No. 3:15-CV-855-SMY-RJD (S.D. Ill. Nov. 11, 2019), ECF No. 575.

[311] Order Granting in Part and Denying in Part Defendant's Motion to Dismiss, *S.D. v. Hytto Ltd., D/B/A/ Lovense*, No. 18-cv-00688-JSW (N.D. Cal. May 15, 2019), ECF No. 44.

[312] Letter Order, *White v. Samsung Electronics America, Inc.*, No. 17-01775 (D.N.J. Aug. 21, 2019), ECF No. 104.

[313] *Id.* at 5.

[314] *Id.* at 6–7.

[315] *See* Defendant Samsung Electronics America, Inc.'s Brief in Support of Motion to Reconsider or, in the Alternative, Motion to Certify Order of August 21, 2019 for Interlocutory Appeal, *White v. Samsung Elec. Am., Inc.*, No. 17-01775 (MCA) (SCM) (D.N.J. Sept. 4, 2019), ECF No. 105-1; Notice of Defendant Sony Electronics Inc. Joining Defendant Samsung Electronics America, Inc.'s Motion to Reconsider or, in the Alternative, Motion to Certify Order of August 21, 2019 for Interlocutory Appeal, *White v. Samsung Elec. Am., Inc.*, No. 17-01775 (MCA) (SCM) (D.N.J. Sept. 4, 2019), ECF No. 106.

[316] *See* First Amended Class Action Complaint and Demand for Jury Trial at 2, *B.F. and A.A. v. Amazon.com, Inc.*, No. 2:19-cv-00910 (W.D. Wash. July 8, 2019), ECF No. 24; Amended Class Action Complaint and Demand for Jury Trial, *R.A. v. Amazon.com, Inc.*, 2:19-cv-06454-CJC-AGR (C.D. Cal. Sept. 18, 2019), ECF No. 42.

[317] First Amended Class Action Complaint and Demand for Jury Trial at 8, 18–33, *B.F. and A.A. v. Amazon.com, Inc.*, No. 2:19-cv-00910 (W.D. Wash. July 8, 2019).

[318] Notice of Voluntary Dismissal, *R.A. v. Amazon.com, Inc.*, 2:19-cv-06454-CJC-AGR (C.D. Cal. Dec. 6, 2019), ECF No. 45; Notice of Voluntary Dismissal by Plaintiffs A.A., B.F., S.M., C.M., and F.B., *C.O. v. Amazon.com, Inc.*, 2:19-cv-910-RAJ-MLP (Dec. 10, 2019), ECF No. 95.

[319] Defendants' Motion to Dismiss Plaintiffs' Second Amended Complaint at 1, *B.F. and A.A. v. Amazon.com, Inc.*, No. 2:19-cv-910-RAJ-MLP (W.D. Wash. Jan. 9, 2020), ECF No. 106.

[320] Order re Motions to Dismiss, *McDonald v. Kiloo APS*, 17-cv-04344-JD (N.D. Cal. May 22, 2019), ECF No. 270.

[321] *Id.*

[322] Scheduling Order, *McDonald v. Kiloo APS*, 17-cv-04344-JD (N.D. Cal. Dec. 19, 2019), ECF No. 316.

[323] Final Judgment, *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, No. 2:17-cv-07232-ODW (JCx) (C.D. Cal. July 8, 2019), ECF No. 101.

[324] Joint Motion to Dismiss, *St. Paul Fire & Marine Ins. Co. v. Rosen Hotels & Resorts, Inc.*, No. 18-14427 (11th Cir. Dec. 27, 2019).

[325] Joint Motion to Dismiss, *The Nat'l Bank of Blacksburg v. Everest Nat'l Ins. Co.*, No. 7:18-cv-00310-GEC (W.D. Va. Mar. 22, 2019), ECF No. 30.

[326] Complaint, *Mondelez Int'l v. Zurich Am. Ins. Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018).

[327] *See* Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong*, N.Y. Times (Apr. 15, 2019), *available at* https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html?login=email&auth=login-email.

[328] Complaint, *Mondelez Int'l v. Zurich Am. Ins. Co.*, No. 2018L011008 (Cir. Ct. Ill. Oct. 10, 2018).

[329] *Id.*

[330] *See* David Voreacos et al., *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, Bloomberg (Dec. 2, 2019, 10:01 PM), *available at* https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war; *see also* Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong*, N.Y. Times (Apr. 15, 2019), *available at* https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html?login=email&auth=login-email.

[331] 139 S. Ct. 1041 (2019) (per curiam).

[332] 136 S. Ct. 1540 (2016).

[333] *Alasaad v. Nielsen*, No. 17-cv-11730-DJC, 2019 WL 5899371, at *21 (D. Mass, Nov. 12, 2019).

[334] *Id*. at *8.

[335] *Id*. at *13.

[336] *See* Notice of Appeal, *Alasaad v. Nielsen*, No. 1:17-cv-11730 (D. Mass. Jan. 10, 2020), ECF No. 115; Notice of Appeal, *Alasaad v. Nielsen*, No. 1:17-cv-11730 (D. Mass. Jan. 13, 2020), ECF No. 117.

[337] *In the Matter of Residence in Oakland, California*, 354 F. Supp. 3d, 1010, 1013 (N.D. Cal. 2019).

[338] *Id*.

[339] *Id*. at 1016 (citing *Doe v. United States*, 487 U.S. 201, 219 (1988) (Stevens, J., dissenting); *Fisher v. United States*, 425 U.S. 391, 420 (1976)); *see also In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012) (holding that decryption and production of hard drives would implicate the Fifth Amendment privilege); *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (holding that subpoena requiring defendant to provide password violated the Fifth Amendment); *Securities and Exchange Commission v. Huang*, No. 15-269, 2015 WL 5611644 (E.D. Pa. Sept. 23, 2015) (holding that passcodes to defendant's work-issued phone is not corporate record and forcing him to produce personal passcodes violates the Fifth Amendment).

[340] *In the Matter of the Search Warrant Application for the Cellular Telephone in United States v. Anthony Barrera*, No. 19 CR 439, 2019 WL 6253812, at *7 (N.D. Ill. Nov. 22, 2019).

[341] *Id*. at *3 (internal quotations and citations omitted).

[342] *Id*.

[343] 18 U.S.C. § 2713.

[344] *Id.*; White Paper, Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the Cloud Act,* 4, 6 (April 2019), *available at* https://www.justice.gov/dag/page/file/1153436/download.

[345] Press Release, Department of Justice, *U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online* (Oct. 3, 2019), *available at* https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

[346] *Id.*

[347] *See* Coalition Statement to U.S. House, Senate Committees Re: U.S.-U.K. CLOUD Act Agreement (Oct. 29, 2019), *available at* https://epic.org/privacy/intl/USUK-CLOUD-Act-Letter-20191028.pdf.

[348] Press Release, European Commission, *Criminal Justice: Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence* (Sept. 25, 2019), *available at* https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890.

[349] Press Release, Department of Justice, *Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton* (Oct. 7, 2019), *available at* https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

[350] White Paper, Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the Cloud Act*, 3 (Apr. 2019), *available at* https://www.justice.gov/dag/page/file/1153436/download.

[351] *See, e.g.*, Katitza Rodriguez & Camille Fischer, *A Race to the Bottom of Privacy Protection: The US-UK Deal Would Trample Cross Border Privacy Safeguards*, Electronic Frontier Foundation (Oct. 4, 2019), *available at* https://www.eff.org/deeplinks/2019/10/race-bottom-privacy-protection-us-uk-deal-would-trample-cross-border-privacy; Press Release, *EPIC, NGOs Object to U.S.-U.K. CLOUD Agreement, Urge Congressional Action*, Electronic Privacy Information Center (Oct. 29, 2019), *available at* https://epic.org/2019/10/ngos-object-to-us-uk-cloud-agr.html.

[352] Office of the Dir. of Nat'l Intelligence, *Release of Documents Related to the 2018 FISA Section 702 Certifications* (Oct. 8, 2019), *available at* https://www.intel.gov/index.php/ic-on-the-record-database/results/951-release-of-documents-related-to-the-2018-fisa-section-702-certifications.

[353] Office of the Dir. of Nat'l Intelligence, *Release of Documents Related to the 2018 FISA Section 702 Certifications* (Oct. 8, 2019), *available at* https://www.intel.gov/index.php/ic-on-the-record-database/results/951-release-of-documents-related-to-the-2018-fisa-section-702-certifications.

[354] *Id.*

[355] Complaint at 1–2, *Am. Civil Liberties Union et al. v. United States Dept. of Justice et al.*, No. 1:19-cv-12242 (D. Mass. Oct. 31, 2019).

[356] Am. Civil Liberties Union Director, T*he FBI is Tracking Our Faces in Secret. We're Suing* (Oct. 31, 2019*), available at* https://www.aclu.org/news/privacy-technology/the-fbi-is-tracking-our-faces-in-secret-were-suing/.

[357] Complaint at 2, *Am. Civil Liberties Union et al. v. United States Dept. of Justice et al.*, No. 1:19-cv-12242 (D. Mass. Oct. 31, 2019).

[358] Saira Hussain, Elec. Frontier Found., *ICE's Rapid DNA Testing on Migrants at the Border Is Yet Another Iteration of Family Separation* (Aug. 2, 2019*), available at* https://www.eff.org/deeplinks/2019/08/ices-rapid-dna-testing-migrants-border-yet-another-iteration-family-separation.

[359] Complaint at 5 & 7, *Elec. Frontier Found. v. United States Dep't of Homeland Sec.*, No. 3:19-cv-07431 (N.D. Cal. Nov. 12, 2019).

[360] Complaint at 2, *Am. Civil Liberties Union et al. v. United States Dept. of Justice et al.*, No. 1:19-cv-12242 (D. Mass. Oct. 31, 2019).

[361] *Id.* at 3.

[362] *Id.*

The following Gibson Dunn lawyers assisted in the preparation of this client update: Ryan Bergsieker, Alexander Southwell, Timothy Loose, Roscoe Jones Jr., Ashley Rogers, Daniel Rauch, Reuben Aguirre, Jennifer Bracht, Chris Connelly, Meghan Dunn, Sarah Erickson-Muschko, Cassandra Gaedt-Sheckter, Julie Hamilton, Doriel Jacov, Nicole Lee, Reid Rector, Jacob Rierson, Isabella Sayyah, Jeremy Smith, Danny Weiner, and Lisa Victoria Zivkovic.

Gibson Dunn's lawyers are available to address any privacy or cybersecurity concerns your business may face. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity and Consumer Protection practice group:

Privacy, Cybersecurity and Consumer Protection Group:

United States
Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Europe
Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 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)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@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 also may be addressed to the following practice leaders:

Securities Regulation and Corporate Governance Group:
Elizabeth Ising - Washington, D.C. (+1 202-955-8287, eising@gibsondunn.com)
James J. Moloney - Orange County, CA (+ 949-451-4343, jmoloney@gibsondunn.com)

GIBSON DUNN

Lori Zyskowski - New York (+1 212-351-2309, lzyskowski@gibsondunn.com)

Related Capabilities

Privacy, Cybersecurity, and Data Innovation