GIBSON DUNN

January 28, 2021

U.S. CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2021

To Our Clients and Friends:

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

2020 was a year of tremendous upheaval and disruption; the privacy and cybersecurity space was no exception. The COVID-19 pandemic, which continues to devastate communities worldwide, raised new and challenging questions about the balance between data protection and public health. Unprecedented cyberattacks by, among others, foreign state actors, highlighted vulnerabilities in both the private and public sectors. Sweeping new privacy laws were enacted, and came into effect. The full ramifications of these changes and challenges are extraordinary, and stand to impact almost every person and company in the country.

This Review places these and other 2020 developments in broader context, addressing: (1) the regulation of privacy and data security, including key updates related to the COVID-19 pandemic, other legislative developments, enforcement actions by federal and state authorities, and new regulatory guidance; (2) trends in civil litigation around data privacy 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 2020, 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 2020 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 this Review; for further details, please see the endnotes.

TABLE OF CONTENTS

I. REGULATION OF PRIVACY AND DATA SECURITY

A. Biden Administration and Presidential Transition

1. Data Privacy
2. Consumer Protection

B. COVID-19 and Privacy

1. Federal Regulatory Efforts
2. State Regulatory Efforts

C. Legislative Developments

1. State Legislative Developments
2. Federal Legislative Developments

D. Enforcement and Guidance

1. Federal Trade Commission
2. Department of Health and Human Services and HIPAA
3. Securities and Exchange Commission
4. Other Federal Agencies
5. State Attorneys General and Other State Agencies

II. CIVIL LITIGATION

A. Data Breach Litigation

B. Computer Fraud and Abuse Act (CFAA) Litigation

C. Telephone Consumer Protection Act (TCPA) Litigation

D. California Consumer Privacy Act (CCPA) Litigation

E. Illinois Biometric Information Privacy Act (BIPA) Litigation

F. Other Notable Cases

III. GOVERNMENT DATA COLLECTION

A. Collection of Cell Phone Data

B. Extraterritorial Warrants and Data Transfers

C. Other Notable Developments

IV. CONCLUSION

I. REGULATION OF PRIVACY AND DATA SECURITY

A. Biden Administration and Presidential Transition

The year 2021 brings with it a new administration under President Biden and a potential shift from the deregulatory priorities often pursued under President Trump. With a closely divided Congress, defined by extremely narrow Democratic majorities in the House and Senate, much of the movement on the legislative and regulatory front may depend on the new administration's ability to find common ground for bipartisan efforts; however, we do anticipate ramped-up legislation, regulation, and enforcement efforts in the data privacy and consumer protection space under the Biden administration.

1. Data Privacy

Republican and Democratic policymakers alike have recognized the need for federal privacy legislation, but persistent differences in approach have foiled efforts to enact a comprehensive legislative scheme so far. Key points of contention around potential federal legislation have included whether and to what extent that legislation should preempt more stringent state laws and whether the legislation should include a private right of action. But as momentum builds among states to enact increasingly stringent data privacy and breach notification laws, so too does the pressure on policymakers seeking to enact meaningful privacy legislation at the federal level. For example, and as we detail further at Section I.C.1., California voters passed an initiative last November to strengthen existing legislation through the California Privacy Rights and Enforcement Act of 2020, and several other states have similar bills in committee at their state legislatures.[1] And, as state privacy laws become more rigorous, it may be more difficult for federal legislation to preempt those state laws entirely because the federal framework would need to be that much more stringent.

That said, the Democratic Party Platform on which President Biden ran provides some additional insight into potential legislative initiatives of the new administration. For example, the platform indicates that President Biden intends to renew the Consumer Privacy Bill of Rights, originally proposed by President Obama, which would seek to add strong national standards protecting consumers' privacy rights.[2] The Platform also indicates that President Biden intends to prioritize updating the Electronic Communications Privacy Act (ECPA) to afford protections for digital content equaling those for physical content.[3]

Policymakers on both sides of the aisle also have expressed concern about Section 230 of the Communications Decency Act and, in particular, the scope of immunity that courts have accorded to social media companies under the statute. The Department of Justice (DOJ) has proposed revisions to the law, including significant limitations on immunity.[4] It is unclear, however, whether legislators will be able to agree on the scope of changes to that immunity, with Republicans voicing concerns about

perceived anti-conservative bias in the ways that social media companies self-regulate speech and Democrats raising concerns about the spread of misinformation and hate speech.

Outside of ongoing legislative efforts, the Biden administration's short-term focus likely will center on administrative action, including promoting federal investigations and enforcement, issuing informal guidance, and initiating formal rulemaking relating to privacy. Such activity would be consistent with Vice President Harris's background as former Attorney General of California and her previous privacy enforcement efforts, including the creation of California's Privacy Enforcement and Protection Unit.[5]

With respect to such federal regulatory enforcement action, it is worth noting that the Federal Trade Commission (FTC) had, at the end of the Trump administration, a Republican Chairman and a 3-2 Republican majority. Yet after President Biden took office, FTC Chairman Joseph Simons announced he would resign effective January 29, 2021, clearing the way for President Biden to appoint a Democratic commissioner and designate a new chair.[6] Further, insofar as FTC Commissioner Rohit Chopra has been nominated as permanent Director of the Consumer Financial Protection Bureau (CFPB), a further FTC vacancy may soon need to be filled.[7]

In the health care arena, we have seen a recent focus on patient privacy rights under HIPAA. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) announced more than a dozen settlements related to "right of access" provisions under HIPAA during the past year, which we discuss further herein at Section I.D.2. The Biden administration has indicated a desire to continue to promote patient control and use of data, and likely will continue to focus on "right of access" enforcement actions.

Beyond the federal level, states remained active in bringing enforcement actions regarding data security and data breach response throughout the Trump administration's term. Given the strong ties that President Biden and Vice President Harris each have to state Attorneys General,[8] cooperation between federal and state enforcement authorities is likely to increase even further under the Biden administration.

2. Consumer Protection

The Consumer Financial Protection Bureau (CFPB), an agency formed during the Obama administration in 2010 following the financial crisis, saw decreased enforcement activity under the Trump administration, in part because President Trump replaced the Bureau's original director in 2017. Since President Biden took office, however, former CFPB director Kathy Kraninger stepped down at the President's request, and Dave Uejio, who previously served as CFPB's strategy program manager, took over as the CFPB's acting director. President Biden has also nominated current FTC Commissioner Rohit Chopra to serve as the permanent CFPB director, a nomination the Senate is expected to consider soon.[9]

On another note, in early 2020 Congress passed, and President Trump signed into law, the Coronavirus Aid, Relief and Economic Security Act (CARES Act), which, among other things, provided forgivable loans to small businesses and placed payment forbearance obligations on financial institutions for mortgage and student loan borrowers and other prohibitions on negative credit reporting due to the COVID-19 pandemic.[10] The CARES Act small business loans were extended by Congress in

December. The Biden administration could seek to enact into law additional COVID-19 stimulus legislation to supplement already-existing laws; indeed, President Biden has already called for a $1.9 trillion stimulus package.[11] In the short term, and particularly as the COVID-19 pandemic continues to have devastating economic impacts on millions of Americans, CFPB enforcement will likely entail closer monitoring of banks and financial institutions for compliance with the CARES Act, especially related to ensuring compliance with the small business loan provisions.

In addition, the Biden administration likely will bring several Obama-era priorities back into focus, including regulation of payday lenders, student loan servicers, affordable credit, credit reporting, and discriminatory lending practices against minority borrowers.[12] Federal-state cooperation is likely here as well, and such cooperation already has begun. In September 2020, for example, the FTC partnered with three other federal agencies and 16 states to conduct "Operation Corrupt Collector" in an effort to challenge debt-collection practices.[13] We anticipate these kinds of enforcement partnerships to continue under the Biden administration.

B. COVID-19 and Privacy

1. Federal Regulatory Efforts

i. Two COVID-19 Privacy Bills Introduced in Congress

In May of 2020, during the last Congress, federal lawmakers introduced two competing privacy bills aimed at protecting privacy interests related to data collection in connection with the COVID-19 response.

The COVID-19 Consumer Data Protection Act (CCDPA), introduced by Senator Jerry Moran (R-KS), requires companies under the jurisdiction of the FTC to obtain affirmative consent for data collection processes related to tracking the spread of COVID-19.[14] The bill would have covered geolocation data, proximity data, and personal health information related to tracking COVID-19 spread; applications measuring compliance with social distancing guidelines; and contact tracing efforts. Additionally, the bill outlined definitions for data deidentification standards and would have established security requirements for companies collecting covered data.

The bill would only have applied for the duration of the COVID-19 health emergency, as declared by the Secretary of Health and Human Services,[15] and it would have established an exclusion for employee health data collected for COVID-19 workplace safety. Importantly, the CCDPA would have expressly preempted existing state laws with respect to COVID-19 data. Proponents of the bill suggested that this would have allowed companies to strike the right balance between individual privacy and innovation, but others argued it would have resulted in less protection for people in states, such as California or Illinois, where current state laws may already provide broader privacy protections.[16] The CCDPA also lacked a private right of action; only the FTC and state Attorneys General would have had enforcement power.

Alternatively, Senator Richard Blumenthal (D-CT) introduced the Public Health Emergency Privacy Act (PHEPA) in an effort to regulate entities that use contact tracing and digital monitoring tools to stop the

spread of COVID-19.[17] Like Senator Moran's bill, PHEPA called for requiring user consent and reasonable data security practices. Unlike the CCDPA, however, Senator Blumenthal's proposal would not have preempted existing state privacy laws, would have created a private right of action, and would have applied to government entities in addition to private businesses.[18] Additionally, the bill would have required federal agencies to report on the potential impact of data collection on civil rights, and would have expressly barred using the data to restrict any individual's right to vote.

Ultimately, neither bill moved forward in the last Congress, and so to the extent such proposals remain salient in 2021 (the 117th Congress), they would need to be reintroduced.

ii. HIPAA Guidance and Enforcement Discretion in Response to COVID-19

In response to the challenges presented by the pandemic, the Federal Government, through the Department of Health and Human Services Office for Civil Rights (OCR), has relaxed HIPAA enforcement and issued new guidance to reassure companies assisting in the fight against COVID-19.

In March 2020, OCR announced it would exercise its enforcement discretion and not impose penalties for noncompliance against health care providers "in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency."[19] OCR subsequently extended that discretion to violations associated with good faith disclosures to public health authorities and participation in COVID-19 testing sites.[20]

That same month, OCR also issued new guidance to ensure HIPAA compliance in the wake of COVID-19. This guidance addressed how covered entities may disclose protected health information to law enforcement, paramedics, and other first responders so as to comply with HIPAA and still facilitate the sharing of real-time information to keep themselves and the public safe.[21] Additional guidance addressing how health care providers may identify and contact recovered COVID-19 patients about blood and plasma donation without violating HIPAA followed in June.[22]

iii. CDC Vaccination Program's Data Use and Sharing Agreement

The Centers for Disease Control (CDC) Vaccination Program Interim Playbook includes a data sharing plan that asks states to provide personal information from residents as part of the CDC's vaccine distribution program.[23] Personal information requirements include recipient name, address, date of birth, and other datapoints, which has raised concerns around the security of the CDC's data systems and use of the information for non-vaccination purposes (although most states have signed onto the data sharing agreement).[24]

2. State Regulatory Efforts

As states look to technological solutions to mitigate the spread of COVID-19, protecting consumer data is at the forefront of many legislators' minds. In 2020 many states considered laws that would have limited how contact tracing apps and individual contact tracers could use, store, and share location data. To date, though, very few states have passed such measures. New York also has introduced a

broader privacy bill that covers the security obligations of many different classes of entities that are responding to the COVID-19 pandemic.[25] In addition, as discussed below, state Attorneys General have been reaching out to corporations to address privacy concerns the pandemic may have exacerbated. We detail recent state legislative initiatives below.

i. Enacted State Laws

California. California enacted AB 713 in September 2020. Although not a direct response to COVID-19, the bill's exemption of certain forms of deidentified health data from the California Consumer Privacy Act (CCPA) may aid in COVID-19 research.[26] AB 713 exempts certain information from the CCPA, provided it is: (1) deidentified under HIPAA; (2) derived from medical information; and (3) not subsequently reidentified. It also "except[s] information that is collected for, used in, or disclosed in research" from the CCPA,[27] which could lower the cost of compliance for health care researchers already complying with HIPPA and increase access to data for further COVID-19 research.

AB 713 also allows for the reidentification of deidentified data for a "HIPAA covered entity's treatment, payment, or health care operation"; public health purposes; and research.[28] It also permits reidentification of data to test or validate a data deidentification technique, but only if the contract for that work bans any other uses or disclosures of the information and requires the return or destruction of the information when the contract ends.[29]

In addition, the bill requires that any business that sells or discloses deidentified patient information disclose in its privacy policy that it does so and that it identify which deidentification method it uses.[30] It also requires that contracts for the sale or license of deidentified information include a requirement that the purchaser or licensee may not further disclose the information to any third party not contractually bound by the same or stricter standards, as well as contractual terms prohibiting reidentification.[31]

Kansas. Kansas is one of the few states to have passed a COVID-19 privacy bill, HB 2016. Unlike other contact tracing bills, it specifically rejects the use of cell phone location data for contact tracing. HB 2016 specifies that contact data, or "information collected through contact tracing," including "medical, epidemiological, individual movement or mobility, names, or other data," shall only be used "for the purpose of contact tracing and not for any other purpose," and may not be disclosed for any reason besides contact tracing.[32] The bill further states that the data should be destroyed when no longer needed for tracing efforts, and that participation in contact tracing is voluntary. It also requires that contact tracers not obtain contact tracing information from a third party, unless the affected party consents or the information was obtained pursuant to a valid warrant. HB 2016 is slated to expire May 1, 2021.

New York. New York recently passed S8450C / A10500C, which limits law and immigration officials from accessing contact tracing information, acting as contact tracers, or receiving information from contact tracers. That law also requires individuals to give "written, informed and voluntary" consent to waive confidentiality and limits the disclosure to the purposes listed in the waiver.[33]

ii. State Laws under Consideration

Alabama. Alabama legislators prefiled a COVID-19 privacy bill, SB1, for their 2021 legislative session. SB1 would prohibit the use of contact tracing data for any other purpose. The bill authorizes the Alabama State Health Officer to adopt rules to implement the act, including defining the types of data that may be collected. With respect to retention, the data must be destroyed "when no longer necessary for contact tracing," but the act does not set out a specific schedule for deletion.[34] SB1 provides a private right to enjoin violations of the statute, and knowing violations of the act would constitute a class C misdemeanor.[35] In its current form, SB1 has a repeal date of May 1, 2022.

New Jersey. New Jersey's COVID-19 bill, A4170, covers contact tracing efforts using both verbal interviews and Bluetooth or GPS services and provides a framework for how contact tracing information may be used, who may have access to it, how it may be stored, and for how long. It also outlines penalties for violations of the bill's usage and deletion guidelines.[36] Information gained from contact tracing efforts may only be used for that purpose and must be deleted from both the public health entity's records and the records of any third party with whom the information is shared within 30 days of its collection.[37] The public health entity also would be required to list the third parties with whom it shares information on the public health entity's website.

Third parties who use the contact tracing information for purposes other than contact tracing, or who fail to delete information in the time specified, are subject to a civil penalty of up to $10,000.[38] The Commissioner of Health would be required to publish proposed guidance on how data collected from contact tracing may be used by public health officials and third parties and how those entities will be required to ensure the security and confidentiality of the data, including any auditing provisions, within 30 days of the effective date of the act.

New York. In 2020, New York legislators, including State Senator Kevin Thomas (a past sponsor of a comprehensive New York data privacy bill[39] and proposed amendments to New York's data breach notification law),[40] introduced S8448D / A10583C, an act "relat[ing] to requirements for the collection and use of emergency health data and personal information and the use of technology to aid during COVID-19."[41] This bill would have applied to a wide set of "covered entities," including "any person, including a government entity[,] that collects, processes, or discloses emergency health data … electronically or through communication by wire or radio," as well as any entity that "develops or operates a website, web application, mobile application, mobile operating system feature, or smart device application for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID-19 public health emergency."[42]

S8448D / A10583C would have required all covered entities to obtain informed, opt-in consent before collecting or using any "emergency health information," defined as "data linked or reasonably linkable to an individual, household, or device … that concerns the public COVID-19 health emergency." This category would have included, for example, genetic, geolocation, demographic, contact tracing, or device information. Further, the act would have imposed strict limits on how and for what purpose covered entities could have processed, shared, or retained such emergency health data.

In terms of information security, the act would have required covered entities to implement reasonable security procedures and practices. It also would have required all covered entities to undergo regular data protection audits—conducted by third-parties—to assess if they had lived up to any promises made to consumers in their privacy notices. Such audits also would have been charged with assessing the relative benefits and costs of the technology a covered entity utilized, along with "the risk that the technology may result in or contribute to inaccurate, unfair, biased, or discriminatory decisions."[43] Finally, the act would have authorized New York's Attorney General to undertake enforcement actions and impose "civil penalties up to $25,000 per violation or up to four percent of annual revenue."[44] In the 2020 legislative session, S8448D / A10583C passed a vote in the New York State Senate. At the start of the 2021 session, the New York State Senate and New York State Assembly each reintroduced versions of the bill.[45]

iii. State Laws Not Enacted

California. California considered two 2020 bills, AB 660 and AB 1782, that aimed to preserve the privacy of data gathered through contact tracing, but neither made it out of the California Senate Appropriations Committee.

AB 660 sought to "prohibit data collected, received, or prepared for purposes of contact tracing from being used, maintained, or disclosed for any purpose other than facilitating contact tracing efforts."[46] It also sought to prohibit any law enforcement official from engaging in contact tracing and required deletion of all information collected through contact tracing within 60 days, except for when in the possession of a health department.[47] The proposed bill also included a private right of action for injunctive relief and attorneys' fees.

AB 1782, the Technology-Assisted Contact Tracing Public Accountability and Consent Terms (TACT-PACT) Act, was a broader bill aimed at businesses engaging in technology-assisted contact tracing (TACT). Under the bill, such businesses were to "provide a simple mechanism for a user to revoke consent for the collection, use, maintenance, or disclosure of data and permit revocation of consent at any time."[48] The bill also would have required any businesses not affiliated with a public health entity to disclose that fact conspicuously. The TACT-PACT Act sought to require businesses or public health entities offering TACT to issue public reports at least every 90 days containing certain information, such as the "number of individuals whose personal information was collected, used, or disclosed pursuant to TACT," and the categories and recipients of the information.[49] The bill also would have imposed encryption requirements for information collected using TACT and provided that the California Attorney General, district attorneys, city attorneys, and members of the public could bring civil actions against businesses for relief from violations of this act's provisions.[50]

Minnesota. Introduced in June 2020, Minnesota's HF 164 would have authorized contact tracing using electronic means and would have prohibited mandatory tracking or mandatory disclosure of health status; further, that law would have forbidden mandatory health tracking by employers. HF 164 would have allowed any person "aggrieved by a violation of this section" to bring a civil action where they could have been awarded "up to three times the actual damages suffered due to the violation," punitive damages, costs and attorney fees, and injunctive or other equitable relief the court deems

appropriate.[51] HF 164 did not become law in the 2020 session, and has not been subsequently reintroduced.

Ohio. Ohio bill HB 61 / SB 31 sought to establish guidelines for all future contact tracing efforts but failed to pass that state's senate. This failed bill specified that contact tracing is voluntary, that information acquired during contact tracing is not a public record, and that consent is requisite to beginning any contact tracing.[52]

iv. State Attorneys General and COVID-19 Privacy

State Attorneys General Joint Letter. In June of 2020, approximately 40 Attorneys General sent a joint letter to two large technology companies regarding the companies' effort to develop an application programming interface (API) for public health authorities to use in creating contact tracing applications.[53] The Attorneys General raised concerns that entities other than public health authorities might use this new API in ways that could "pose a risk to consumers' privacy." The Attorneys General therefore called on the companies to: (1) verify that any contact tracing application using this API was, in fact, affiliated with a public health authority; (2) remove from their mobile-app marketplaces those apps that could not be so verified; and (3) remove all contact tracing applications from their respective mobile-app marketplaces at the end of the COVID-19 national emergency.[54]

New York Consent Agreement with Videoconferencing Business. Despite requests from industry groups to delay enforcement due to COVID-19, New York began enforcement of the Stop Hacks and Improve Electronic Data Security (SHIELD) Act in March of 2020. A videoconferencing software made more popular during the pandemic was the first target of a SHIELD-like enforcement action, one that yielded a significant consent decree.[55] Although not technically brought under the SHIELD Act, the consent decree included many provisions aimed at ensuring compliance with the Act's mandates, including requirements to maintain a comprehensive data security program involving regular security risk assessments, to report those assessments to the office of the New York Attorney General, and to enhance encryption protocols. The videoconferencing business also agreed to stop sharing user data with social media companies and to give videoconference hosts more control over outside access to videoconferences.[56]

C. Legislative Developments

1. State Legislative Developments

i. California

a. California Consumer Privacy Act (CCPA)

Effective January 1, 2020, the California Consumer Privacy Act (CCPA) aims to give California consumers increased visibility into and control over how companies use and share their personal information. The CCPA applies to all entities that conduct business in California and collect California consumers' personal information if those entities meet certain thresholds relating to their annual revenue or volume of data processing.[57]

Despite initially passing in 2018 and coming into effect early in 2020, the CCPA has continued to evolve throughout 2020, as reported in detail in Gibson Dunn's prior CCPA updates.[58] On August 14, 2020, California Attorney General Xavier Becerra announced that the state's Office of Administrative Law approved the final CCPA regulations.[59] The approved regulations—which took effect immediately on August 14, 2020—largely track the final regulations proposed by the Attorney General on June 1, 2020, and include regulations focused on key definitions, notices to consumers, business practices for handling consumer requests, verification of requests, special rules regarding consumers under 16 years of age, and anti-discrimination rules.[60]

On October 12, 2020 and December 10, 2020, Attorney General Becerra submitted additional modifications to the regulations, clarifying the opt-out requirement for the sale of personal information.[61] Specifically, these modifications reintroduce the requirement that businesses that substantially interact with consumers offline must provide an offline notice of a consumer's ability to opt out of the sale of personal information. In addition, the modifications reintroduce language requiring that the methods used by businesses for submitting requests to opt out "be easy for consumers to execute" and "require minimal steps to allow the consumer to opt-out." The modifications also provide a uniform opt-out button companies may choose to use.[62]

b. California Privacy Rights and Enforcement Act (CPRA)

On November 3, 2020, only four months after the CCPA became enforceable by the California Attorney General, Californians voted in favor of California Proposition 24, and with it, the California Privacy Rights and Enforcement Act (CPRA), which further amends but does not replace the CCPA. Of note, the CPRA will become law *as written* and cannot be readily amended by the state legislature. Instead, any significant changes to the law would require further voter action. Although the CPRA will not go into effect until January 1, 2023, it provides consumers with rights relating to personal information collected during the prior 12 months, thus extending the CPRA's reach to personal information collected on or after January 1, 2022. The CCPA will remain in full force and effect, as previously drafted, until the effective date of the further amendments under the CPRA.

As reported in Gibson Dunn's prior CPRA updates,[63] the CPRA expands upon the CCPA in granting the right to limit the use of consumers' sensitive personal information, the right to correct personal information, the right to data minimization, and a broader right to opt out of the sale of personal information; in imposing requirements and restrictions on businesses, including new storage limitation requirements, restrictions on automated decision-making, and audit requirements; and in expanding breach liability. The CPRA also amends the definition of covered "businesses" by increasing the threshold number of consumers or households (and eliminating the consideration of "devices" from this number)[64] from 50,000 to 100,000 (exempting certain smaller businesses)[65] and broadening the threshold percentage of annual revenue to also include revenue derived from *sharing* personal information.[66] Further, it expands the definition of "publicly available information" to include information "that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media," as well as "information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the

information to a specific audience."[67] The CPRA also expands the definition of "selling" to expressly include sharing and cross-context behavioral advertising.[68]

Additionally, the CPRA establishes an entirely new enforcement agency—the California Privacy Protection Agency (CPPA)—that will have co-extensive enforcement authority with the California Attorney General. The CPPA will have administrative enforcement authority, while the Attorney General will have civil enforcement authority to impose civil penalties of up to $2,500 per violation or $7,500 per intentional violation or violation involving a minor's protected personal information.

ii. Other States' Laws

Aside from the CPRA, several other states considered, passed, or began enforcement on their own data privacy and consumer protection laws in 2020, though to date none have been as far-reaching as those of California.

a. Maine

Maine's "Act To Protect the Privacy of Online Customer Information" went into effect July 1, 2020.[69] The Act prohibits Internet providers from using, disclosing, selling or permitting access to customer personal information unless the customer consents, and the provider may not refuse to serve a customer or penalize a customer that does not consent.[70] The Act does provide for some exceptions from obtaining customer consent—specifically, for the purpose of providing the service, advertising the Internet provider's own services, protecting against fraudulent or unlawful use of the services, providing emergency services, and facilitating payment.[71]

b. Nevada

On October 1, 2019 Nevada's "Act relating to Internet privacy" went into effect, requiring website operators to permit consumers to opt out of the sale of personal information to third parties.[72] However, as of this writing there has not been news of any enforcement under this law.

A second Nevada privacy law came into effect on January 1, 2021, in the form of amendments to NRS 603A.210 that require government agencies maintaining records that contain personal information about Nevada residents to comply with the current version of the Center for Internet Security Controls or corresponding standards adopted by the National Institute of Standards and Technology of the United States Department of Commerce.[73] Furthermore, the amendment requires Nevada's Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration to create and make available a public list of controls with which the state must comply.[74] Additionally, before disposing of electronic waste, Nevada's courts must first permanently remove any data stored on such objects.[75]

c. New York

As noted previously, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) went into effect in March of 2020.[76] The SHIELD Act amends the state's existing data breach

notification law to impose an affirmative duty on covered entities to implement reasonable data security to protect the "private information" of New York residents (with a more flexible standard for small businesses).[77] To provide "reasonable data security," a person or business that collects or maintains the private information of New York residents must implement a data security program with specified administrative, technical, and physical safeguards, including disposal of data after that data is no longer necessary for business purposes and designating an employee to oversee the data security program.[78] The Act, however, specifies that entities that are compliant with certain federal statutes, such as the Gramm-Leach-Bliley Act (GLBA) or Health Insurance Portability and Accountability Act (HIPAA) are also deemed compliant with the SHIELD Act.[79] The SHIELD Act grants the Attorney General enforcement authority and the power to bring suit for a failure to provide reasonable data security, but does not allow for private action.[80]

Separately, Governor Cuomo recently proposed a comprehensive New York data privacy bill, titled the "New York Data Accountability and Transparency Act" (NYDAT), as part of his 2021 budget.[81] Similar to the CPRA, NYDAT would grant New York residents the right to request that a business destroy or correct that resident's personal information, as well as the right to opt out of the sale of personal information. The Act would also carry data minimization requirements, and would allow consumers to enforce this and other requirements through a private right of action. Furthermore, NYDAT would create a new data privacy agency, the Consumer Data Privacy Advisory Board, which would be empowered with rulemaking authority.[82]

In prior legislative sessions, comprehensive data privacy bills with even stronger protections have been proposed, such as the New York Privacy Act.[83] That proposal would have imposed on covered entities a "data fiduciary duty," and would have granted New York residents a private right of action for *any* violation of the bill.[84] Given newly-elected Democratic supermajorities in both houses of New York's state legislature,[85] any final NYDAT bill may well end up including some of these heightened protections or broader enforcement mechanisms.

d. Oregon

Oregon's "Act Relating to actions with respect to a breach of security that involves personal information" went into effect January 1, 2020.[86] The Act defines a covered entity as a person that owns, licenses, maintains, stores, manages, collects, processes, acquires, or otherwise possesses personal information in the course of the person's business, vocation, occupation, or volunteer activities.[87] Under the Act, covered entities must notify customers and the Attorney General of any breach of security regarding personal information.[88] The Act amended, broadened, and renamed the Oregon Consumer Identity Theft Protection Act, defined "covered entities," and specifically required vendors to report security breaches.[89] The Act also added usernames (and other methods of identifying a consumer for the purpose of permitting access to a user's account) to the definition of "Personal information."[90] Notably, "Personal information" under the Act includes data from automatic measurements of a consumer's physical characteristics, such as fingerprint, retina, and iris data.[91]

Similarly, Oregon's "Act Relating to security measures required for devices that connect to the Internet" went into effect January 1, 2020.[92] The Act requires manufacturers to equip Internet-connected

devices with "reasonable" security, which may consist of external authentication or compliance with federal law for such devices. This is similar to California's Security of Connected Devices law, which also took effect January 1, 2020.[93]

e. Washington

Washington's "Act relating to the use of facial recognition services," which will go into effect July 1, 2021, regulates the use of facial recognition technology by state and local governments.[94] The Act requires government agencies that intend to develop, procure, or use facial recognition services to specify the purpose of the technology, produce an accountability report, and ensure that decisions made by such a service are subject to human review if they have legal effect. Such agencies are further required to test the service's operational conditions, conduct periodic training of individuals who operate the service or process acquired personal data, and, where information gathered by such services is to be used in prosecutions, disclose use of the service to criminal defendants in a timely manner prior to trial.[95] Furthermore, under the Act, state and local agencies must require their providers of facial recognition services to make available an application programming interface (API) or other technical capability to ensure independent review regarding the accuracy and fairness of performance across subpopulations divided by race and other protected characteristics.[96]

f. Additional State Laws Under Consideration and Local Laws Passed

A number of other states continued to consider passing comprehensive privacy laws, both in 2020 and at the start of 2021. In Washington State, for instance, Senator Reuven Carlyle has released the draft Washington Privacy Act 2021 for review and public comment,[97] which marks the third introduction of the Washington Privacy Act. The draft Act seeks to provide consumers the right to access, correct, and delete personal data, and to opt out of collection and use of personal data for certain purposes.[98] Furthermore, the Act would seek to protect use of personal and public health data during the global pandemic as technological innovations emerge, especially in relation to contact tracing.[99]

Several other states also considered biometric privacy legislation in 2020, including Massachusetts, Hawaii, and Arizona.[100] On this point, a growing number of municipalities passed laws or ordinances in 2020 that banned or limited the use of facial recognition technology, including Boston, Pittsburgh, Oakland, San Francisco, Portland (Maine), and Portland (Oregon).[101] Pittsburgh, for its part, enacted a law that limits police use of facial recognition to instances in which its city council finds that acquisition, retention, and use of such technology does not perpetuate bias or pose risks to the civil rights and liberties of residents.[102] Portland, Oregon's ban, meanwhile, is the first to limit *private* businesses' use of facial recognition technology in public places—that ordinance went into effect January 1, 2021.[103] Diverging privacy protections granted across states (and cities) will continue to pose serious questions for businesses navigating this complex compliance environments.

2. Federal Legislative Developments

i. Comprehensive Privacy Legislation

As the patchwork of federal, state, and local privacy regulations grows more complex, comprehensive federal privacy legislation remains a popular, but elusive goal, often divided along partisan lines.[104] Democratic legislators, in general, favor federal privacy legislation that includes a private right of action, while Republicans tend to favor legislation that explicitly preempts state privacy laws.[105] With a Democratic administration and (narrow) Democratic majorities in Congress, the chances of passing federal privacy legislation may be greater now than in past years. At the same time, because many states and cities have made noteworthy legislative developments in 2020 (as outlined above), Democratic legislators may feel less incentive to compromise on a federal privacy law if it means accepting federal preemption of such state- and city-level efforts.[106]

In any case, with the 2020 election behind us, 2021 may well see a renewed push for a comprehensive federal privacy law. Several bills introduced during 2020, as discussed below, provide insight into the type of legislation we may see in the months and years ahead. But it remains to be seen which, if any, of these approaches will gain traction in 2021, particularly as any such bills from the last Congress would need to be reintroduced in the current one.

a. Republican-Backed Legislation

The Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act),[107] introduced in the last Congress by Senator Roger Wicker (R-MS)—the leading Republican on the Senate Commerce, Science, and Transportation Committee—has been called the "strongest piece of [privacy] legislation put forth by Senate Republicans to date."[108] Introduced and referred to the Committee on Commerce, Science, and Transportation in September 2020, the SAFE DATA Act was largely an updated version of the U.S. Consumer Data Privacy Act (CDPA), which had been introduced by Republicans towards the end of 2019.[109] The SAFE DATA Act also drew upon two prior bipartisan proposals—the Filter Bubble Transparency Act,[110] and the Deceptive Experiences To Online Users Reduction Act (DETOUR Act).[111] Key features of the SAFE DATA Act included: (1) requiring companies to obtain express consent before processing sensitive data or using personal data for behavioral or psychological studies; (2) providing users with the right to access, correct and delete their data, as well as data portability; (3) requiring companies to notify users if personal data is used with an "opaque" algorithm to select content that the user sees, and to offer users a version of the platform that uses an "input-transparent" algorithm instead; and (4) creating a victims' relief fund within the Treasury Department to provide consumers with monetary relief for privacy violations.[112] The bill remained consistent with the two pillars of other Republican-backed efforts by expressly preempting state laws and many federal laws, and by not providing for a private right of action.[113]

Senator Jerry Moran (R-KS) also introduced the Consumer Data Privacy and Security Act of 2020 (CDPSA),[114] which would have provided for the broad preemption of all related state and local laws, and would not have included a private right of action.[115] This bill was referred to the Committee on Commerce, Science, and Transportation in March,[116] but did not become law.

b. Democratic-Backed Legislation

The Data Broker Accountability and Transparency Act of 2020 (DATA Act) was introduced in the House and referred to the House Committee on Energy and Commerce in May,[117] though the last Congress did not enact it as law. This proposal was the House version of a bill introduced in the Senate in September 2019.[118] The DATA Act would have provided individuals with a right to access their data, dispute that data's accuracy, and opt out of the use of their data for marketing purposes.[119] Additionally, the Act would have required data brokers to inform consumers on how to exercise their rights, and establish procedures to ensure the accuracy of collected personal information.[120] However, it did not include a private right of action—enforcement would have been left to the FTC and to state Attorneys General.[121]

Additionally, Senator Kirsten Gillibrand (D-NY) introduced the Data Protection Act of 2020 to create an independent national Data Protection Agency (DPA) that would have been empowered to promulgate rules and initiate enforcement actions to protect individual privacy—thus taking enforcement out of the FTC's hands.[122] In particular, the bill's supporters were concerned that a comprehensive federal privacy law without a private right of action could leave the FTC alone to enforce privacy rights, "which [Democrats] are convinced would lead to weak enforcement."[123] Senator Gillibrand's bill would have worked to address this concern by creating a new independent agency tasked with enforcing individual privacy rights instead.[124] The DPA would have had the authority to investigate and issue subpoenas against covered entities on its own initiative, or individual consumers could have themselves brought complaints and requests to the DPA.[125]

Finally, last June Senator Sherrod Brown (D-OH), the top Democrat on the Senate Banking, Housing, and Urban Affairs Committee, released a discussion draft of the Data Accountability and Transparency Act of 2020.[126] Although it was not formally introduced in the last Congress, the Act was noteworthy in that rather than depend on the usual consent-based privacy framework that requires users to agree to privacy policies to use online services, this proposal would have completely banned the collection, use and sharing of personal data in most circumstances.[127] Additionally, it would have outlawed facial recognition technology and would have created a new agency with enforcement authority to protect privacy.[128]

c. Bipartisan-Backed Legislation

The Application Privacy, Protection and Security Act of 2020 (APPS Act)[129] was one of the only bipartisan comprehensive privacy laws proposed in the last Congress. First introduced in 2013, the APPS Act was reintroduced by Representative Hank Johnson (D-GA) and cosponsored by Representative Steve Chabot (R-OH).[130] It was referred to the House Committee on Energy and Commerce in May,[131] though it ultimately failed to become law. The APPS Act would have established new rules governing the collection and use of consumer data by applications on mobile devices.[132] It would have required developers to take "reasonable and appropriate measures" to secure personal data from unauthorized access, although it did not offer standards for what would be considered "reasonable."[133] The proposal would also have required developers to provide specific information on the types of data that the application collects, the purpose of the collection, and the

developer's data retention policy.[134] Consumers, in turn, would have been given the right to opt out of data collection and delete previously collected data.[135] The APPS Act would only have preempted state laws that directly conflicted with it or provided a lower "level of transparency, user control, or security" than the APPS Act itself.[136] Finally, the proposal would not have provided a private right of action—instead, it would have been enforced by the FTC and by state Attorneys General.[137]

ii. Other Federal Legislation

In addition to the comprehensive privacy proposals considered in 2020, additional federal legislation was proposed, and in some cases enacted, on narrower and more specific topics related to data privacy and cybersecurity. Below are proposals that gained traction in 2020 or that may gain legislative momentum in 2021.

a. Internet of Things Cybersecurity Improvement Act

The Internet of Things Cybersecurity Improvement Act of 2020 (IoT Cybersecurity Improvement Act) was signed into law by President Trump on December 4, 2020.[138] The Act mandates certain security requirements for IoT devices purchased by the federal government.[139] These guidelines will be issued by the Office of Management and Budget, consistent with the National Institute of Standards and Technology's (NIST) recommendations.[140] NIST will be tasked with working with the Department of Homeland Security to create these guidelines to help ensure that federal government devices and networks are secure from malicious cyberattacks.[141]

b. Biometric and Facial Recognition Legislation

Three federal legislative proposals were introduced in 2020 regarding the use of biometric and facial recognition technology. In part because this technology has been shown to disproportionately misidentify women and people of color,[142] legislators, and particularly Democratic legislators, have prioritized this space in order to better ensure equity and protect individuals' privacy and safety. While none were enacted in the last Congress, each reflects the increased emphasis placed on this issue:

- The Ethical Use of Facial Recognition Act was introduced by Senators Jeff Merkley (D-OR) and Cory Booker (D-NJ), and would have placed a moratorium on the use of facial recognition technology by the federal government until Congress passed legislation regulating its use.[143]

- The Facial Recognition and Biometric Technology Moratorium Act of 2020 was a bicameral proposal[144] that would have barred federal government use of biometric technology, a ban which could only be lifted through a subsequent act of Congress.[145] The bill included a prohibition on the use of such data in judicial proceedings and a private right of action for individuals whose data is used in violation of the Act.[146] Senators Bernie Sanders (I-VT) and Elizabeth Warren (D-MA) co-sponsored the Senate proposal,[147] while the House bill was co-sponsored by seventeen Democratic House members.[148]

- The National Biometric Information Privacy Act of 2020 was introduced in the Senate by Senators Jeff Merkley (D-OR) and Bernie Sanders (I-VT).[149] The bill would have prohibited

private companies from collecting biometric data without consumer or employee consent.[150] Additionally, it would have limited the ability to retain, buy, sell and trade biometric information without written consent.[151] The bill would have been enforced by state Attorneys General, as well as by individuals through a private right of action.[152]

c. Lawful Access to Encrypted Data Act

The Lawful Access to Encrypted Data Act was a Republican bicameral proposal that would have required device manufacturers and service providers to assist law enforcement in accessing encrypted data if a proper warrant were obtained, and which would have directed the United States Attorney General to create a prize competition to award participants who create a lawful access solution to an encrypted environment.[153]

d. USA FREEDOM Reauthorization Act of 2020

In March 2020, as discussed in more detail at Section III.B., three Foreign Intelligence Surveillance Act (FISA) authorities lapsed: (1) Section 215 of the USA Patriot Act, also known as the "business records" provision;[154] (2) the "lone wolf" authority;[155] and (3) the "roving wiretap" authority.[156] Initially, this appeared to provide an opportunity for changes to be made to FISA, and the Senate passed several bipartisan FISA amendments aimed at strengthening various privacy protections.[157] However, the House rejected these amendments, and as of this writing, these authorities continue to remain lapsed unless and until the current Congress reauthorizes them.

e. Attempts to Weaken Section 230 of the Communications Decency Act

Under Section 230 of the Communications Decency Act (Section 230)[158] online platforms and technology companies are shielded from liability for content posted by certain third parties.[159] Several legislative proposals in the last Congress directly aimed at curtailing this immunity, and while none became law, similar efforts will almost surely be made in 2021.[160] Key 2020 bills included:

- The Limiting Section 230 Immunity to Good Samaritans Act (Good Samaritans Act) was introduced by Senator Josh Hawley (R-MO) in June of 2020.[161] That bill would have required companies that want to receive Section 230 immunity to contractually bind themselves to a duty of good faith when enforcing their terms of service in order to avoid discriminatorily applying such terms, or risk a $5,000 fine per violation.[162] Sponsoring senators stated that the bill's goal was to decrease technology companies' ability to silence conservative political speech.[163]

- Senate Judiciary Chairman Lindsey Graham (R-SC) and bipartisan co-sponsors introduced the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (EARN IT Act).[164] Upon introduction, the EARN IT Act was referred to the Committee on the Judiciary, where it was unanimously approved.[165] On July 20, the proposal was placed on the Senate Legislative Calendar.[166] As of November, the EARN IT Act had a total of sixteen bipartisan co-sponsors,[167] though ultimately the last Congress did not enact it into law. The proposal

would have established a national commission to determine best practices for technology companies to prevent the exploitation of children online. It also would have created an incentive for technology companies to follow those practices by removing Section 230 immunity for child sexual abuse posted on their platforms.[168]

- The Behavioral Advertising Decisions Are Downgrading Services Act (BAD ADS Act) was introduced by Senator Josh Hawley (R-MO) and referred to the Committee on Commerce, Science, and Transportation in July.[169] Had it become law, the BAD ADS Act would have required large technology companies to stop personalized behavioral advertising in order to maintain their Section 230 immunity.[170]

f. Amendments to the Children's Online Privacy Protection Act of 1998

In 2019, the FTC launched a broad review of the Children's Online Privacy Protection Act of 1998 (COPPA)[171] in an effort to modernize the statute and provide greater protections for children online.[172] Two pieces of legislation were proposed in the House in January 2020 to amend and update COPPA as a result of this initiative, though neither ultimately became law.

First, the bipartisan PROTECT Kids Act would have: (1) raised the minimum age under which parental consent must be obtained before a company can collect personal data from 13 to 16 years old; (2) clarified that COPPA applies to mobile applications; and (3) added geolocation and biometric data as categories of personal data protected under COPPA.[173] Second, the Democratic-supported PRIVACY Act would have modified requirements for commercial entities with respect to information collected from children under 13, and "young consumers" under 18 years old.[174] For example, it would have required: (1) securing such information and periodically testing security measures; (2) obtaining consent to process such information; and (3) providing consumers the right to access and delete it.[175]

D. Enforcement and Guidance

1. Federal Trade Commission

As in past years, in 2020 the Federal Trade Commission (FTC) was one of the federal government's foremost enforcers in the area of privacy and data security. In this section, we discuss the FTC's robust enforcement actions during 2020. We also preview an important legal challenge for the FTC at the Supreme Court, where the Court is poised to resolve a split among the Circuit Courts of Appeals regarding the FTC's authority to seek monetary relief under Section 13 of the FTC Act.[176]

i. Data Security and Privacy Enforcement

The FTC pursued a number of significant enforcement, and related, actions in 2020 relating to data privacy.

Section 6(b) Study Related to Social Media and Video Streaming Companies. In mid-December, the FTC issued orders to nine major technology companies, requiring them to provide the FTC with information regarding how the companies collect, use, and present personal information; their advertising and user engagement practices; and how their practices affect minors.[177] The FTC issued these orders under Section 6(b) of the FTC Act, which gives the FTC authority to conduct broad studies without first identifying a specific law enforcement purpose. These types of studies typically lead to reports and potentially legislative proposals.

Landmark Settlement. In April, the U.S. District Court for the District of Columbia approved a landmark $5 billion settlement with a major technology company over allegations by the FTC that the company misled users into thinking certain settings would protect their information, including pictures and videos, when instead such information was allegedly shared by the company with advertisers and other third parties.[178] In a statement at the time, FTC Chairman Joe Simons indicated that the settlement was "by far the largest monetary penalty ever obtained by the United States on behalf of the FTC and the second largest in any context."[179]

Significant Consent Breach Settlement. In August, a major social media platform announced that it expects to pay up to $250 million to resolve charges by the FTC that the company had breached a 2011 consent decree by using data that users provided for security purposes, such as phone numbers and email addresses, to target such users with advertisements.[180] The company initially entered into the 2011 consent decree, which remains in effect until 2031, after hackers were able to gain unauthorized control over users' accounts on the company's platform, including access to some users' private messages.

Cybersecurity Practices Settlement. In November, the FTC announced a major, albeit nonmonetary, settlement with a leading digital communications company over allegations that the company engaged in unfair and deceptive practices by issuing misleading statements regarding the company's cybersecurity practices.[181] The FTC alleged that the company represented to users that it used end-to-end encryption on all teleconferences, when in fact it only used such encryption when a call was hosted on a customer's server. The FTC also alleged that the company advertised itself as using 256-bit encryption despite actually using a lower level of encryption; that the company advertised that it immediately encrypted and stored teleconference recordings when in fact such recordings remained unencrypted for 60 days; and that the company circumvented certain browser privacy safeguards and failed to disclose this circumvention.

Children's Privacy Consent Decree. In July, media reports indicated that the FTC was investigating the developer of a popular social media application for alleged violations of a 2019 consent decree geared toward protecting children's privacy.[182] The consent decree required the company to delete videos and personal information relating to users under the age of 13. The FTC has not yet commented on the investigation, but two unidentified individuals have reported being interviewed by the FTC in connection with this investigation.

ii. Supreme Court to Rule on FTC's Monetary Relief Authority

The FTC typically seeks monetary relief in privacy and cybersecurity actions under Section 13(b) of the FTC Act, which states that, "Whenever the Commission has reason to believe … that any person, partnership, or corporation is violating, or is about to violate any provision of law enforced by the Federal Trade Commission[,]" the Commission may seek "a temporary restraining order or a preliminary injunction[.]"[183] As discussed in last year's Review, despite the lack of any express reference to monetary remedy or relief, the FTC views its authority to recover monetary relief under Section 13(b) as well settled. But in 2019, the Court of Appeals for the Seventh Circuit created a circuit split by holding in *FTC v. Credit Bureau Center, LLC*[184] that Section 13(b) does not authorize the FTC to seek monetary awards, breaking with eight other circuits and with its own prior precedent. The Seventh Circuit reached this decision by relying on the textualist observation that Section 13(b) "authorizes only restraining orders and injunctions,"[185] and although the court conceded that it had previously "endorsed [the FTC's] starkly atextual interpretation," it ultimately determined that "[s]tare decisis cannot justify adherence to [that] approach."[186]

In July, the U.S. Supreme Court granted certiorari[187] in a related case, *AMG Capital Management, LLC v. FTC*,[188] to resolve whether Section 13(b) does confer the authority to impose monetary awards.[189] In *AMG*, the Ninth Circuit affirmed an approximately $1.27 billion equitable monetary award the FTC obtained under Section 13(b) against a payday lender. Although the Ninth Circuit observed that Plaintiff's argument regarding the FTC's authority to obtain monetary judgments under Section 13(b) "ha[d] some force," it concluded such an argument was "foreclosed by our precedent."[190] Should the Supreme Court ultimately hold that the FTC lacks such authority, the ruling could have seismic implications on how the FTC goes about enforcing federal data privacy and security laws, an outcome that would likely lead to new legislation.

2. Department of Health and Human Services and HIPAA

As discussed above, in 2020 the Department of Health and Human Services (HHS) grappled with unprecedented patient privacy challenges caused by the COVID-19 pandemic. While HHS continued to conduct investigations and issue civil penalties for violations of the Health Insurance Portability and Accountability Act (HIPAA), it also allowed for some leniencies, especially with regard to telehealth regulations. The Office for Civil Rights (OCR) at HHS was particularly active in 2020 through its new HIPAA Right of Access Initiative, which it launched toward the end of 2019. The OCR settled more than a dozen Right of Access Initiative investigations in 2020, with entities ranging from hospital systems to solo practitioners—all in an effort to ensure patients have timely and affordable access to their own medical records.

Also to that end, in December 2020, HHS OCR proposed significant changes to the HIPAA Privacy Rule via a Notice of Proposed Rulemaking (NPRM). These proposed changes seek to increase patients' access to their electronic health information, advance the state of coordinated health care, and reduce the regulatory burdens on the healthcare industry more broadly. These developments are further addressed below.

i. HHS OCR Enforcement

In 2020, the OCR continued to enforce privacy protections for patients through investigations and settlements, especially as part of its Right of Access Initiative. 2020 also saw the second-largest settlement in OCR's history ($6.85 million paid by a large health insurer). However, the numerous smaller-dollar settlements that the OCR reached with a diverse range of health care entities, including solo practitioners and non-profits, tend to reflect HHS's "high-volume, low-penalty focus" as announced in April 2019.[191] The following are notable HIPAA-related settlements from 2020:

Large Health Insurer Malware Attack. The largest settlement of the year, at $6.85 million, involved a large regional health insurer that was subject to a malware attack that compromised the health data of over 10 million individuals. The attack was perpetrated using a phishing email that gained access to the insurer's IT system. The OCR investigation found "systemic noncompliance with the HIPAA Rules including failure to conduct an enterprise-wide risk analysis, and failures to implement risk management, and audit controls."[192] The insurer agreed to two years of monitoring, in addition to the monetary penalty.

Low Penalty Settlements. As part of HHS OCR's recent "high-volume, low-penalty focus," HHS OCR also reached multiple settlements with individual health care providers and other smaller entities. As one example, a Utah-based solo practitioner settled with the OCR for $100,000 following an investigation that revealed a "failure to implement basic HIPAA requirements."[193] This case, and other similarly small settlements reached in 2020, demonstrate that HHS is increasingly interested in ensuring HIPAA compliance at all levels of the health care sector.

Right of Access Settlements. HHS also reached a number of settlements under the Right of Access Initiative, which is intended to enforce HIPAA provisions aimed at ensuring patients have access to their own medical records. As just one example, a small psychiatry office in Colorado agreed to pay $10,000 to the OCR in response to a complaint that it had failed to comply with the HIPAA Privacy Rule's right of access provision. Many of the other Right of Access Initiative settlements in 2020 involved similarly low monetary settlement amounts, with the focus instead being placed on corrective action.[194]

ii. Involvement by State Attorneys General

In recent years, state Attorneys General have been increasingly involved in enforcing HIPAA regulations, a trend which continued in 2020. Most notably, in September, a 43-state coalition of Attorneys General reached a settlement with a major health insurer over the largest health data breach in United States history, which occurred between December 2014 and January 2015. The insurer's $39.5 million settlement with the Attorneys General followed its record-setting $16 million settlement with the OCR in 2018,[195] and the approval, also in 2018, of a $115 million class action settlement in the Northern District of California.[196] We expect that state Attorneys General will continue taking an active enforcement and investigatory role with respect to health care data privacy protections going forward.

iii. COVID-19 Regulations and Guidance

The pandemic has raised many challenging patient privacy issues, requiring HHS to balance the desire for robust privacy protections with the necessity of timely and widespread access to testing and care. HHS has been active in issuing guidelines in response to the novel issues posed in 2020, as demonstrated by the following:

- ***Patient-Provider Communications***. In March 2020, HHS announced it would "exercise its enforcement discretion and … waive potential penalties for HIPAA violations against health care providers that serve patients through everyday communications technologies during the COVID-19 nationwide public health emergency."[197] This Notification of Enforcement Discretion (NDE) cleared providers for the good faith use of videoconferencing services, such as FaceTime and Skype, when communicating with patients remotely. The NDE currently has no expiration date.[198]

- ***COVID-19 Testing Sites***. In April 2020, HHS announced it would not impose penalties "for violations of the HIPAA Rules against covered entities or business associates in connection with the good faith participation in the operation of COVID-19 testing sites during the COVID-19 nationwide public health emergency."[199] This NDE allowed those companies and agencies equipped to facilitate COVID-19 testing to launch efforts without being stalled by the need to ensure robust HIPAA protections.

- ***Blood and Plasma Donation***. In June 2020, HHS issued guidance that "covered health care providers [can] contact their patients who have recovered from COVID-19 to inform them about how they can donate their blood and plasma containing antibodies to help other patients with COVID-19."[200] In August 2020, the Trump administration amended this guidance to further provide that hospitals, pharmacies, laboratories, and health plans may also contact recovered patients about blood donation.[201]

iv. Request for Public Comments on HHS's Notice of Proposed Rulemaking (HIPAA Privacy Rule)

On December 10, 2020, HHS announced an NPRM with respect to HIPAA's Privacy Rule as part of its Regulatory Sprint to Coordinated Care initiative. The initiative, launched under HHS Secretary Alex Azar, broadly seeks to "promote value-based health care by examining federal regulations that impede efforts among health care providers and health plans to better coordinate care for patients."[202]

The currently proposed changes to HIPAA, in particular, would facilitate increased patient and caregiver access to medical records, as well as decrease regulatory barriers to information sharing between providers for the purposes of care coordination and case management.[203] The NPRM was published in the Federal Register on January 21, 2021, and stakeholders have until March 22, 2021 to submit comments.[204]

3. Securities and Exchange Commission

The Securities and Exchange Commission (SEC) is increasingly focused on digital practices and risks, as evidenced by its recent guidance on privacy and cybersecurity and its prioritization of information security issues. For example, a review of SEC enforcement actions in 2020 shows that cryptocurrency and initial coin offerings remained a central focus for the Commission. The Commission also filed two enforcement actions related to web-based market manipulation schemes. That said, the SEC announced no new enforcement actions related to account intrusions, hacking, or cybersecurity controls and safeguarding customer information in 2020.

i. Data Privacy Guidance and Examination Priorities

On January 7, 2020, the SEC's Office of Compliance Inspections and Examinations (OCIE) released its 2020 Examination Priorities for registered firms.[205] The Priorities make clear that companies could face regulatory action if they materially understate their digital risks, avoid discussing significant incidents they have already experienced, or publicly overstate their data security or privacy practices. The Priorities emphasize that registrants' use of non-traditional sources of data from inputs like mobile device geolocations, consumer credit card records, and other Internet-based information, will be a particular focus of examination review.[206] The Priorities also establish that OCIE will prioritize cyber and other information security risks.[207]

On January 27, 2020, OCIE also issued guidance regarding data loss prevention policies, scrutiny of third-party vendors, and the use of detailed and routinely tested incident response plans to prepare for issues in the cybersecurity space.[208] This guidance prominently features data loss prevention policies, and recommends that firms regularly scan for vulnerabilities in their systems, establish patch management programs, and screen for insider threats by monitoring suspicious activity.

Further, on July 28, 2020, the SEC announced the creation of a new specialized unit within OCIE designed to rapidly respond to current market threats and critical matters.[209] In light of the SEC's increased focus on digital risks, this Event and Emerging Risks Examination Team (EERT) was specifically tasked with addressing cybersecurity incidents (in addition to other significant market events that could have a systemic impact or that place investors assets at risk).

ii. Cryptocurrency

The SEC also focused substantial enforcement resources on combatting unregistered or fraudulent initial coin offerings (ICOs) to the public, filing no fewer than 23 individual enforcement actions related to digital assets or ICOs in the 2020 calendar year.[210] Two cases were particularly significant because the courts affirmed an expansive interpretation of the SEC's regulatory authority:

- On June 26, 2020, the SEC won a cryptocurrency enforcement decision before the U.S. District Court for the Southern District of New York, ultimately resulting in an $18.5 million civil penalty.[211] Addressing the plaintiff's earlier motion for a preliminary injunction, the court found that the digital assets in question were, in fact, subject to applicable securities laws, and that the SEC had shown a substantial likelihood of success in proving that the defendants had

engaged in an unregistered offering of securities in their sale of digital tokens to investors.[212] By focusing on "economic reality" and piercing through contractual representations and warranties to decide whether a token sale should be regulated under the securities laws, the court articulated a broad interpretation of the SEC's enforcement authority.[213]

- Similarly, on September 30, 2020, U.S. District Court for the Southern District of New York gave the SEC another significant victory, this time against a mobile messenger application company, alleging that the company had engaged in an unregistered offer and sale of digital asset securities. The Court again emphasized the "economic realities" of the transactions at issue and found that under the Supreme Court's test in *SEC v. W.J. Howey Co.*,[214] the company's token sales were a single integrated offering and so needed a registration statement.[215]

In addition to obtaining these significant decisions, the Commission filed many other cryptocurrency-related actions over the course of the year, with claims ranging from defrauding investors to engaging in unauthorized sales of securities.[216] This underscores the emphasis the Commission continues to place on enforcement in this area.

iii. Web-Based Market Manipulation

2020 also saw the SEC zero in on web-based market manipulation concerns. For example, towards the beginning of the year, the Commission filed a complaint against a Russian national (and entities he controlled) for allegedly participating in a plot to lure investors into purchasing fictitious certificates of deposit promoted through internet advertising and "spoofed" websites that imitate the actual sites of legitimate financial institutions.[217] On December 23, 2020, the Court entered default judgment for the SEC based on the defendants' failure to respond.[218] Likewise, later in 2020, the Commission filed charges against a former day trader for his alleged role in a market manipulation scheme in which he and several other individuals fabricated online rumors about publicly traded companies in order to trade around the temporary price increases caused by the dissemination of the false information.[219] Taken together, these developments suggest that web-based manipulation will also be an important area of enforcement (consistent with the Commission's renewed focus on cybersecurity and data integrity discussed above).

4. Other Federal Agencies

In addition to the FTC, HHS, and SEC, other federal government entities continue to make headlines in the data security, privacy, and consumer protection space. This past year, there were notable developments at the Federal Communications Commission (FCC), the Department of Justice (DOJ), the Department of Defense (DoD), and the Department of Transportation (DOT).

i. Federal Communications Commission

a. Telephone Consumer Protection Act

While COVID-19 has slowed down many federal agencies, the pandemic has not impacted the pace of enforcement related to the Telephone Consumer Protection Act (TCPA). Indeed, new developments continue to arise daily at the time of this writing.

Under the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), passed in December of 2019, the Federal Communications Commission (FCC) was required to clarify exemptions to the TCPA by December 30, 2020.[220] To that end, the FCC has now issued a Notice of Proposed Rulemaking[221] that could bring about substantial changes to TCPA enforcement—including making certain classes of non-commercial calls to residential phone lines, which were previously exempt, actionable under the TCPA.[222]

Additionally, two major cases involving interpretation and enforcement of the TCPA are currently making their way through the federal court system. The U.S. Supreme Court heard oral arguments in *Facebook, Inc. v. Duguid* on December 8, 2020—a case centered on a dispute over the definition of the term "autodialer" under the TCPA.[223] Additionally, in *Carlton & Harris Chiropractic Inc. v. PDR Network, LLC*, the Fourth Circuit set up another TCPA issue that may ultimately reach the Supreme Court when it ruled that FCC interpretation of portions of the TCPA is not subject to *Chevron* deference, as had been widely assumed.[224] District courts have given the FCC strong deference with respect to their interpretations of the TCPA for over a decade;[225] however, the result of *PDR Network*—if it stands—would allow courts to apply a much more relaxed form of deference, and to more frequently override the FCC's interpretations of the TCPA.

b. Enforcement against Telecommunications Firms

In addition to its rulemaking function, the FCC has continued to actively enforce privacy and consumer protection laws under its purview. In late February 2020, for example, the FCC handed down over $200 million in fines against several of the nation's major mobile carriers.[226] The fines resulted from a 2017 investigation into Securus, a prison phone company, which revealed that company's plans to share users' real-time location tracking information—obtained from the major mobile carriers—with law enforcement.[227] Press reports later confirmed that customer information from mobile carriers ended up in the hands of law enforcement officers without a warrant or any other valid legal orders.[228]

ii. Department of Justice

Although the DOJ has not traditionally played a leading role in enforcing privacy, cybersecurity, or consumer protection laws, in 2020 the DOJ took action significantly implicating all three areas.

First, in October 2020, the DOJ announced that it was moving forward with a high-profile antitrust investigations into the country's largest technology companies. In what will likely become the largest antitrust lawsuit in more than two decades, the DOJ took aim at the tech industry and sued a large search engine platform and technology business.[229] Attorney General William Barr accused the search

engine of using "its monopoly power … to lock up key pathways to search on mobile phones, browsers, and next generation devices [such] that no one can feasibly challenge [the search engine's] dominance."[230] Just two months later, the DOJ's suit against the search engine was followed by federal and state antitrust cases against a large social media company, alleging similarly anticompetitive behavior.[231] We will continue to monitor the progress of both lawsuits throughout 2021 and beyond as a new Attorney General inherits these current actions from the previous administration.

Second, also in October, the DOJ made statements on two emerging technologies with privacy implications—encryption and cryptocurrency—sharing concerns about both. Both technologies have become widely used in numerous industries and have afforded users a newfound ability to protect the privacy of their data online.

On October 1, 2020, the DOJ published a comprehensive, 83-page strategy outlining the Department's attitude towards cryptocurrency—both the underlying blockchain technology itself and the more esoteric markets for trading various forms of cryptocurrency.[232] In the report, the DOJ revealed an intention to litigate perceived abuses in both domestic and international cryptocurrency exchanges.

Later that month, the Attorney General co-signed a statement from the law enforcement branches of seven nations—the United States, the United Kingdom, Australia, New Zealand, Canada, India, and Japan—urging the tech "industry to address [the governments'] serious concerns" about end-to-end encryption.[233] In this statement, the DOJ called on tech companies to "include mechanisms in the design of their encrypted products and services [to allow governments to] gain access to data in a readable and usable format."[234] While the debate about including a "backdoor" to encrypted devices and data has been raging for over a decade, this joint statement signals increased government pressure on companies to include such an ability, or else to curtail the use of end-to-end encryption in consumer devices entirely.[235]

iii. Department of Defense

On December 1, 2020 the DoD's Cyber Maturity Model Certification (CMMC) finally came into effect after a rule change was delayed earlier in the year.[236] CMMC now requires that all contractors with the DoD achieve one of five levels of cybersecurity, based on the sensitivity of the contracted-for products and services.[237] Furthermore, CMMC has created a board of certified accreditors who will test all potential DoD contractors to determine their level of cybersecurity.[238] Companies must receive the proper CMMC accreditation before signing future contracts with the DoD. This represents a fundamental shift for the agency, whose cyber policy used to simply require contractors to self-certify compliance with a given standard of security.[239]

iv. Department of Transportation & National Institute of Standards and Technology

On January 8, 2020 the DOT published Ensuring American Leadership in Automated Vehicles 4.0 (AV 4.0) which laid out the federal government's position towards the development and deployment of autonomous vehicles.[240] The report focused on three key areas: (1) the U.S. Government autonomous vehicle (AV) principles; (2) administration efforts supporting AV technology growth and leadership;

and (3) U.S. Government activities and opportunities for collaboration.[241] While the report offered many suggestions for safety, security and privacy, AV 4.0 stopped short of issuing any concrete regulations.[242] However, the Department signaled that more concrete regulations may be on the horizon when it issued an Advance Notice of Proposed Rulemaking on November 23, 2020.[243]

The National Institute of Standards and Technology (NIST) also released two concurrent publications in May that provide guidance on cybersecurity precautions that manufacturers should incorporate into all devices with Internet connectivity[244]—part of the IoT Cybersecurity Improvement Act,[245] as referenced above in Section I.C.2. This guidance will encourage companies to implement appropriate security measures by evaluating the device in connection with its user interactions and other systems that the device may interact with.

5. State Attorneys General and Other State Agencies

As evident from the above discussions, state Attorneys General continued their work in the data privacy and cybersecurity space throughout 2020, often collaborating to bring enforcement actions involving large-scale data breaches, as well as consumer protection actions aimed at regulating the technology industry.

i. State Attorneys General Enforcement Actions

Health Insurance Company. As noted above, in September 2020, a health insurance company agreed to pay $39.5 million to resolve claims brought by the Attorneys General of 42 states and the District of Columbia after a 2015 data breach exposed personal information of nearly 80 million consumers.[246] The Attorneys General alleged the insurance company violated state laws and HIPAA by not encrypting consumers' personal information.[247] As part of the settlement, the company also agreed to implement a comprehensive security program.[248]

Home Improvement Retailer. A coalition of the Attorneys General of 46 states and the District of Columbia entered into a settlement with a home improvement company in November 2020 over allegations regarding a data breach that compromised the financial information of over 40 million consumers.[249] The Attorneys General claimed that a 2014 data breach allowed hackers to access the payment information of consumers who used the company's self-checkout lanes throughout the United States.[250] Under the settlement, the company agreed to pay $17.5 million and to implement a comprehensive information security program designed to protect and secure the confidentiality of consumers' personal information.[251]

Videoconferencing Platform. As discussed in Section I.B.2, in May 2020, the New York Attorney General's Office entered into a letter agreement with a videoconferencing business that became more popular during the pandemic, settling an investigation into the company's privacy and data security practices.[252] In March, the New York Attorney General's Office began investigating the company's cybersecurity, citing specifically to vulnerabilities that could enable uninvited third parties to interrupt conferences and access consumer webcams.[253] Recognizing the cooperation of the videoconferencing platform in the investigation, the agreement was focused mainly on forward-looking, rather than punitive, remedies, such as requiring the company to implement new security and privacy

measures, to establish a comprehensive data security program, and to better encrypt users' information.[254]

***Search Engine Platform and Technology Company*.** The Arizona Attorney General filed a complaint against a search engine platform and technology company in May 2020, alleging the company's collection of location data violated the Arizona Consumer Fraud Act.[255] The complaint, filed in Maricopa County Superior Court, specifically alleges that the company continues to collect information regarding users' location even if users turn off the smartphone operating system's digital tracking features.[256] Arizona's Attorney General further alleges that the company misled consumers to believe location tracking was controlled by a single setting, while making other location-tracking settings difficult for users to locate.[257] The court denied a motion to dismiss the complaint in September 2020.[258]

California Attorney General CCPA Enforcement Letters. Despite protests from industry groups seeking additional time for compliance in light of COVID-19, the office of the California Attorney General, as scheduled, began enforcing the California Consumer Privacy Act (CCPA) starting July 1, 2020. This enforcement has thus far consisted of sending out enforcement letters informing businesses of their current non-compliance with the CCPA. Businesses have 30 days from the receipt of such letters to remedy any alleged violations—and failure to do so can lead to a civil action brought by the Attorney General. To date, these letters do not appear to have targeted a particular industry or sector, though this may change during 2021.

New Massachusetts Data Privacy and Security Division. On August 13, 2020, the Massachusetts Attorney General announced the creation of the Data Privacy and Security Division (DPSD) within the Massachusetts Attorney General's office. The Division will focus on investigating and enforcing potential violations of the state's consumer protection and data breach laws.[259]

ii. New York Department of Financial Services

As noted in our 2019 Review, in May 2019, New York's Department of Financial Services (DFS) announced the creation of a Cybersecurity Division.[260]

On July 21, 2020 the DFS joined the ranks of cybersecurity regulators by announcing charges against an insurer for violations of the DFS's cybersecurity regulations.[261] According to the DFS's Statement of Charges and Notice of Hearing, the insurer had an alleged vulnerability in its information system, resulting in the potential exposure of millions of documents containing sensitive personal information.[262] The DFS claims that the insurer knew about the vulnerability but underestimated the level of risk associated with it.[263] The insurer is strongly contesting the charges, noting that only 32 clients may have had their nonpublic information compromised.[264] In any case, this matter should shine some additional light on the expansiveness of DFS's cybersecurity policies and the extent of its authority.[265]

In October 2020, DFS also issued a report criticizing a social media company for becoming prey to a "simple" hacking technique earlier that summer.[266] Hackers accessed accounts of high-profile individuals and companies to send out fraudulent messages, resulting in the unlawful attainment of over

$118,000 of Bitcoin.[267] DFS urged lawmakers to establish a regulator to "monitor and supervise" mainstream social media platforms, arguing the hack demonstrated the dangerous ability to "weaponize" such platforms.[268]

Lastly, on October 15, 2020, DFS announced plans for its first ever "tech sprint" to develop a set of common standards and an open source technical framework to be adopted by DFS and other regulatory agencies with the goal of speeding up collection of supervisory data needed to monitor financial firms.[269] The multi-day event, set for early 2021, will host teams of fintech (financial technology) professionals, compliance experts and others to respond to the need for more up-to-date information about the health of banks and other financial institutions.[270] DFS said it selected cryptocurrency companies as the starting point, with future events in the series to potentially focus on other types of nonbank financial firms.[271]

II. CIVIL LITIGATION

A. Data Breach Litigation

After 2019 was declared "the worst year on record" for data breaches,[272] breaches and other security lapses continued to occur at a high rate in the past year. As COVID-19 forced many people to work remotely, a survey conducted by a cybersecurity company found that remote work led to security breaches at up to 20% of companies surveyed in 2020.[273] Indeed, some of the world's largest businesses experienced data breaches in 2020, including technology giants, hospitality and entertainment chains, and health care companies. Various parts of the United States government also recently were found to have suffered a major, months-long data breach.[274] Unsurprisingly, a number of these breaches have spawned class action or shareholder derivative litigation. The past year also saw several major settlements resolving data breach cases from prior years.

1. Class Action and Shareholder Derivative Litigation

Social Networking Platform. A shareholder derivative lawsuit in the U.S. District Court for the Northern District of California, originating from a March 2018 report that a third party wrongfully obtained information about the users of a large social networking platform, remains ongoing, with an amended complaint filed against the social media company on December 17, 2019.[275] In response to the social media company's renewed motion to dismiss, plaintiffs have argued that their amended complaint now alleges sufficient demand futility based on new information regarding the founder and CEO's control over the company's board. The court has yet to rule on the renewed motion to dismiss.[276]

Online Retailer and Technology Company. In April 2020, the U.S. District Court for the Western District of Washington denied a large retailer and technology company's motion to compel arbitration in a class action discussed in last year's Review.[277] In this case, plaintiffs allege that the company used voice-enabled devices to build a "massive database of billions of voice recordings" containing private information of children without the consent of the children or their parents. The company has since appealed the ruling.[278]

Videoconferencing Provider. In April 2020, a major videoconferencing provider was sued in a putative class action in the U.S. District Court for the Northern District of California for allegedly having "inadequate data privacy and security measures" and making false assertions that its videoconference service was end-to-end encrypted.[279] While the lawsuit does not allege that the company actually suffered any data breach, it does allege security vulnerabilities and cites security-related investigations into the company by the New York and Connecticut state Attorneys General.[280] The lawsuit also alleges that the company's executives impermissibly dumped stock prior to stock price declines caused by disclosures relating to the company's security vulnerabilities.[281] Similar allegations caused the company to reach a settlement with the FTC in November 2020, as well, as discussed in further detail in Section II.D.1.

Two months later, in June 2020, the company, its CFO, and all but one of its nine board members were sued in U.S. District Court for the District of Delaware in a shareholder derivative action.[282] The derivative suit specifically alleges that a number of defendants, including the company's CEO, breached their fiduciary duties and profited from "lucrative insider sales" made while in possession of material nonpublic information about the company's alleged security vulnerabilities.[283]

Clinical Laboratory Company. In April 2020, a company that operates a network of clinical laboratories, along with several of its directors and officers, was sued in the Delaware Court of Chancery in a shareholder derivative action alleging breaches of fiduciary duties relating to two data breaches.[284] The suit alleges that the first data breach resulted in the exposure of credit card information, personally identifiable information, and personal health information, while the second breach resulted in the exposure of further personal health information.[285] The suit also alleges insufficient data security measures and practices and conscious disregard or delay in disclosing the breaches.[286]

Search Engine Platform and Technology Company. On August 7, 2020, a proposed class action lawsuit was filed against a search engine platform and technology company for allegedly recording consumers via the company's connected, voice-activated home devices.[287] The complaint alleges that the company thereby violated the California Invasion of Privacy Act, the California Consumer Privacy Act, as well as the federal Wiretap Act, by recording consumers using sensitive microphones in the company's devices without user consent.[288] The company has moved to consolidate this claim with other pending litigation on a similar issue.[289]

Cloud Computing Company. In August 2020, a cloud computing company was sued in a putative class action in the U. S. District Court for the District of South Carolina.[290] The suit alleges that "negligent conduct" on the part of the defendant made the personal information of the defendant's customers vulnerable to hackers.[291] Specifically, the suit alleges that a three-month ransomware attack, occurring between February and May 2020, exposed the personal information of "students, patients, donors, and other individual users," and that the defendant did not notify the persons whose data had been exposed until July or August 2020.[292] Although the defendant has asserted that social security, credit card, and bank account numbers were not exposed by the breach, the suit alleges that that the defendant "cannot be assured" such data was not exposed.[293]

Financial Services Company. In November 2020, a financial services company and several of its officers and directors were sued in the U.S. District Court for the District of Delaware in a shareholder derivative action alleging Securities Act violations and breaches of fiduciary duties relating to an alleged security flaw that persisted for years before being exposed in May 2019.[294] The suit alleges that publicly accessible URLs hosted by the company exposed customers' sensitive personal information, including names, addresses, birth dates, social security numbers, bank account numbers, and more.[295] The suit alleges that the company failed to remedy this vulnerability even after it was exposed by a penetration test conducted in December 2018.[296] The suit also alleges that the company's CEO profited by selling stock after the vulnerability was detected but before it was publicly exposed.[297]

2. Key Settlements

Technology Company. The U.S. District Court for the Northern District of California approved a $13 million *cy pres* settlement of claims against a major search engine platform and technology company that allegedly gathered information from unencrypted Wi-Fi networks using its geo-mapping car fleet.[298] The settlement, which a class member has appealed to the U.S. Court of Appeals for the Ninth Circuit, includes a $10 million grant to data security charities in lieu of a distribution to class members. Although the district court stated the settlement ultimately benefits class members by protecting their interest in internet security through the work of these charities, the objecting class member is arguing that plaintiffs' counsel breached their duty to class members by negotiating a deal that would provide monetary disbursements to third parties rather than their clients.[299] The Ninth Circuit has yet to rule on the appeal.[300]

Technology Company. In June 2020, the U.S. District Court for the Northern District of California preliminarily approved a $7.5 million class action settlement for claims filed in 2018 relating to data breaches affecting a since-discontinued social media service.[301] The parties agreed to the terms of the settlement in January 2020.[302]

Web Services Company. In July 2020, the U.S. District Court for the Northern District of California approved a $117.5 million class action settlement for claims stemming from data breaches that affected at least 194 million customers between 2012 and 2016.[303] The order approving the settlement is notable due to the detailed analysis evaluating the reasonableness of the settlement, in which the court compared the settlement to another large data breach settlement approved in 2018.[304] The Court used a number of factors, including the per capita recovery and other remedies under the settlement, the multiplicity of the breaches, the time period over which the breaches occurred, the companies' denials regarding the breaches, the companies' promptness in notifying users of the breaches, the sensitivity of the exposed data, and more.[305] These factors may be applied in future data breach cases to determine the reasonableness of settlement terms.

B. Computer Fraud and Abuse Act (CFAA) Litigation

The scope of the Computer Fraud and Abuse Act (CFAA) has divided the federal circuit courts, but some clarity may be on the horizon. The CFAA provides for criminal penalties and private civil remedies

against anyone who accesses a computer "without authorization" or who "exceeds" their "authorized access" to such a computer.[306] Circuit courts are divided over whether a person who is authorized to access information on a computer for *certain* purposes "exceeds authorized access" in violation of the CFAA by accessing the same information, but for other, *unauthorized* purposes. The First, Fifth, Seventh, and Eleventh Circuits have held that the CFAA imposes liability in such circumstances.[307] By contrast, the Second, Fourth, Sixth, and Ninth Circuits have held that the CFAA does not reach such conduct.[308]

On April 20, 2020, the U.S. Supreme Court agreed to hear *Van Buren v. United States*, which may resolve this circuit split.[309] In *Van Buren*, the Eleventh Circuit upheld the CFAA conviction of a Georgia police officer who was paid by an informant to look up license-plate information in a database that could only be used for law-enforcement purposes.[310] The Court agreed to consider whether the officer violated the CFAA when he used that database for an unauthorized purpose.[311] At oral argument in November, the officer's attorney and the government sparred over whether upholding the conviction would create an interpretation of the CFAA that would criminalize common activities, such as employees accessing social media websites while at work. Indeed, Justice Gorsuch warned that a broad interpretation of the CFAA could end up "making a federal criminal of us all" and Justice Sotomayor worried that the CFAA is "dangerously vague."[312] A decision is expected later in 2021.

Although *Van Buren* is a criminal case, its outcome will have implications for civil CFAA cases as well, particularly those involving the collection of information from publicly available websites. In fact, the petitioner in *LinkedIn v. hiQ Labs, Inc.* has urged the Supreme Court to grant its petition for certiorari to address whether other companies may use automated software to "scrape" or harvest large amounts of data from public websites such as the appellant's professional social networking website.[313] The Ninth Circuit held that such automated mass data collection is not a CFAA violation where the information can be collected without circumventing a login or other authorization procedure.[314] The appellant, however, argues that this "scraping" is a CFAA violation because the social networking website denied authorization to data harvesters by sending a cease-and-desist letter and by employing technical measures to thwart such scraping.[315] The Court has not yet acted on the petition.

More targeted efforts at collecting data from public-facing websites have also raised CFAA concerns. One such effort is at issue in *Sandvig v. Barr*.[316] In that case, a group of researchers brought a pre-enforcement challenge in U.S. District Court for the District of Columbia, alleging that the CFAA violated the First Amendment as applied to the researchers' intended conduct of intentionally violating employment websites' terms of service in order to research whether such websites engage in race- or gender-based discrimination. The researchers intended to use fake candidate profiles (a terms of service violation) to test various publicly accessible websites for employment discrimination. The researchers alleged that the CFAA would criminalize such conduct, and thereby violate their First Amendment rights. The trial court concluded that the researchers would risk CFAA liability only if they planned to bypass the websites' authentication mechanisms, such as a requirement to enter a password. Because the planned conduct would not have bypassed such login procedures, the court found the researches would not have violated the CFAA. The court reasoned that "[c]riminalizing terms-of-service violations risks turning each website into its own criminal jurisdiction and each webmaster into his own legislature."[317] The court concluded that, in light of this holding, the researchers' First Amendment

claims were moot. The researchers have appealed the decision, which is currently pending in the D.C. Circuit.[318]

C. Telephone Consumer Protection Act (TCPA) Litigation

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

First, at the start of the year, the Eleventh Circuit joined the Third and D.C. Circuits in adopting a narrow reading of what constitutes an automatic telephone dialing system (ATDS) under the TCPA.[319] The court determined that the TCPA's phrase "using a random or sequential number generator" modifies both the "stor[age]" and "produc[tion]" of numbers.[320] As such, the court found that the TCPA only covers devices that both "store numbers using a random or sequential number generator, or produce such numbers using a random or sequential number generator and dial them."[321] Shortly thereafter, the Seventh Circuit denied a petition for rehearing in a case on this issue, joining the Third, D.C., and Eleventh Circuits in adopting a narrow reading of what amounts to an ATDS under the TCPA.[322]

These rulings deepened the circuit split created by the Ninth Circuit's September 2018 decision in *Marks v. Crunch San Diego, LLC*, which interpreted the TCPA's definition of an ATDS broadly to apply to any equipment with the capacity to store and automatically dial numbers, even if the device cannot itself store or produce the numbers using a random or sequential number generator.[323] In April, the Second Circuit became the first federal appellate court to join the Ninth Circuit in adopting this broad interpretation of autodialers under the TCPA.[324] The Sixth Circuit followed suit a few months later, applying a broad interpretation of ATDS in its decision in *Allan v. Pennsylvania Higher Education Assistance Agency*.[325]

With the scope of the TCPA's definition of ATDS continuing to divide the circuit Courts of Appeal, on July 9, 2020, the Supreme Court granted certiorari in *Facebook v. Duguid*, responding to the social media company's petition filed in late 2019.[326] The case is expected to provide some much-needed clarity as to what constitutes an ATDS under the TCPA. In September, the federal government filed an amicus brief in support of the social media company and joined the company in urging the Supreme Court to reject the Ninth Circuit's broad view of devices subject to the TCPA's autodialer restrictions.[327] The Court heard arguments in early December and is expected to reach a decision by the spring of 2021.[328] Whichever side the Court comes out on, the decision will have drastic implications for TCPA liability. But in any case, the decision is likely to provide businesses currently subject to divergent TCPA standards throughout the country with more concrete direction.

In addition to agreeing to hear *Facebook v. Duguid*, the Supreme Court addressed another aspect of the TCPA in *Barr v. American Association of Political Consultants, Inc.*[329] The Court there upheld the TCPA's sweeping ban on autodialed calls to cell phones, but struck down an exception for calls made to collect federally backed debts, reaching this result on First Amendment grounds.[330] Between a plurality opinion and various concurrences, six justices found that the TCPA's robocall restrictions and the government-debt exception amounted to content-based speech restrictions that were impermissible under the First Amendment.[331] In this view, the TCPA's robocall restriction was content-based

because it favored speech made for purposes of collecting government debt over speech made for political or other important purposes.[332] Justice Sotomayor, acting as the sixth vote to strike down the government exception, agreed that the exception violated the First Amendment, but found that the appropriate standard was intermediate scrutiny, rather than strict scrutiny.[333] With six justices finding the government-debt exception for robocalls unconstitutional, the Court then considered whether to invalidate the TCPA's robocall restriction in its entirety, or to instead sever the government-debt exception while upholding the remainder of the restriction. Applying "traditional severability principles," the Court decided to uphold the TCPA's sweeping ban on robocalls while invalidating and severing the government-debt exception from the remainder of the statute.[334] Given the varied rationales among the Court's plurality and concurring opinions, however, the case's broader First Amendment ramifications remain to be seen.

D. California Consumer Privacy Act (CCPA) Litigation

1. Broadening the Scope of a "Data Breach"

Since the California Consumer Privacy Act (CCPA) went into effect on January 1, 2020, various consumers have filed suits seeking relief for CCPA violations. In particular, the CCPA includes a private right of action in the context of a data breach, allowing consumers, both individually and as a class, to initiate a civil suit when their personal information is subject to an "unauthorized access and exfiltration, theft, or disclosure as a result of the business'[s] violation of the duty to implement and maintain reasonable security procedures and practices."[335] Despite the limited basis for a private right of action under the CCPA, litigants have attempted to enlarge its scope by including CCPA-based claims in such data privacy actions.

Videoconferencing Company. On March 30, 2020, a class action was filed in the federal district court for the Northern District of California against a videoconferencing company.[336] In their original complaint, plaintiffs alleged that the defendant unlawfully shared user data with a social media partner in violation of the CCPA.[337] This case, however, does not allege a conventional data breach claim. Instead, the plaintiffs claimed that the voluntary data sharing arrangement between these companies *itself* constituted a breach.[338] Interestingly, in a recent filing, the plaintiffs dropped this CCPA claim as a distinct cause of action, instead simply asserting the alleged violation in passing.[339] A motion to dismiss has been filed and is currently pending.[340]

Retailers and Loss Prevention Service Provider. On July 7, 2020, a similar class action was filed in the federal district court for the Central District of California against several retail companies and a loss prevention service provider.[341] The plaintiffs' allegations are based on the defendants' voluntary sharing of consumer information with a third-party loss prevention service provider.[342] The plaintiffs alleged that the retailers' sharing of information in an "unsecured, unrestricted manner" to create consumer reports and to generate a risk score which was shared with other defendants resulted in a widespread and unauthorized dissemination of personal information.[343] According to the amended complaint, the plaintiffs claim that the defendants violated the CCPA by: (1) collecting and using personal information without providing consumers with notice; (2) failing to inform users of personal information collected about them and the third parties with whom that information was shared; and (3)

failing to prevent non-encrypted and non-redacted personal information from unauthorized disclosure as a result of the defendants' failure to implement and maintain reasonable security procedures and practices.[344] Notably, the first two violations are not subject to the CCPA's private right of action, which is a trend in CCPA litigation that we cover in further detail below. Many of the retailers have now sought to compel arbitration and dismiss the claims.[345]

2. Expanding the Definition of "Personal Information"

The CCPA establishes a limited private right of action for when a consumer's "nonencrypted and nonredacted personal information" is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures."[346] However, the CCPA's definition of "personal information" for this private right of action is narrower than the definition of "personal information" for the rest of the CCPA, including only: (1) Social Security number; (2) driver's license number or California identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) medical information; or (5) health insurance information.[347] Recently, consumers have attempted to expand the types of information that would be actionable under the CCPA in the case of a data breach. Below, we highlight a salient example:

Software Company. On July 21, 2020, a class action was filed against a software company in the federal district court for the Central District of California.[348] The plaintiffs claimed that sensitive student information was unlawfully accessed after the defendant failed to maintain appropriate data safeguards in accordance with the CCPA.[349] The defendant filed a motion to dismiss, arguing that the plaintiffs' allegations rely on a definition of "personal information" that was beyond the scope of the statute.[350] Specifically, the defendant argued that the CCPA does not protect student information like the "parent name, student name, student ID (School), physical resident address, email address, and password hashes" that were accessed in the case.[351] The court has not yet ruled on the motion to dismiss, and proceedings are currently stayed pending settlement discussions.[352]

3. Litigating Notice and Opt-Out Provisions

The CCPA's larger regulatory scheme notably protects a consumer's right to be notified about a business's collection, use, sharing, or sale of their personal information, and to opt out of having such information sold to third parties.[353] While the California Attorney General is presently tasked with enforcing these broader provisions, consumers are limited to bringing actions for data breach-related claims under Section 1798.150.[354] The text of the CCPA explicitly prohibits private suits involving other provisions of the statute.[355] Nevertheless, litigants have still attempted to enforce the statute's notice and opt-out provisions through private actions.

Videochat Application. On April 17, 2020, a class action was filed in the federal district court for the Southern District of California against the owners of a videochat application.[356] The plaintiffs claimed that the defendants failed to provide adequate notice of the application's data collection activities and did not give consumers the opportunity to opt out of the sale of their personal information, including

opt outs through the required "Do Not Sell My Personal Information" link.[357] The plaintiffs pursued a CCPA violation claim based on the alleged failure to provide notice, even though the CCPA does not provide for a private right of action for these types of claims. On August 4, 2020, the court granted the defendants' motion to compel arbitration.[358]

Social Networking Platform. On May 20, 2020, a similar class action was filed against a social networking platform in the federal district court for the Central District of California.[359] The plaintiffs alleged that the platform's facial recognition technology scanned videos, extracted biometric information, and stored data without notifying users.[360] The plaintiffs argued that the platform violated the CCPA by failing to provide notice and the opportunity to opt out of its third-party disclosure, as well as by collecting, retaining, and using customers' biometric information without notice.[361] The complaint did not address the issue of whether these claims could be litigated in light of the statute's restrictions on suits by private litigants. The case has since been consolidated and transferred to the federal district court for the Northern District of Illinois.[362]

4. CCPA Violations under the UCL

California's Unfair Competition Law (UCL) creates a private right of action for consumers to enjoin and seek restitution for a business act or practice that is "unlawful," "unfair," or "fraudulent."[363] Violations of other statutes can serve as a predicate for a UCL claim. However, the text and legislative history of the CCPA establish that consumers are prohibited from using CCPA violations as the basis for a cause of action under a separate statute, which seems to clearly preclude using the CCPA as the basis for liability under the UCL.[364] Nevertheless, consumers are testing the limits of this restriction.

Facial Recognition Technology Company. On February 27, 2020, a class action was filed against a technology company in the federal district court for the Southern District of California. The plaintiffs claimed that the defendant scraped and sold biometric information without adequate notice to consumers.[365] The plaintiffs therefore alleged that the defendant violated the UCL by failing to provide the appropriate notice under the CCPA.[366] On December 15, 2020, the United States Judicial Panel on Multidistrict Litigation consolidated and transferred the case to the federal district court for the Northern District of Illinois.[367]

Online Marketplace. On June 11, 2020, a class action was filed in the federal district court for the Northern District of California against an online marketplace for artists.[368] The plaintiffs alleged that the defendant's insufficient security procedures breached its duty of care and allowed hackers to access consumer information in violation of the CCPA.[369] The plaintiffs also brought a separate UCL claim predicated on the defendant's alleged unlawful conduct.[370] The parties are currently in arbitration-related discovery.[371]

E. Illinois Biometric Information Privacy Act (BIPA) Litigation

2020 was yet another active year for litigation under the Illinois Biometric Information Privacy Act (BIPA), which creates a private right of action against entities that fail to comply with the statute's requirements for collection and storage of biometric data.[372] Courts examined a variety of issues in

BIPA cases, including standing and preemption by other state statutes. The COVID-19 pandemic also introduced new types of BIPA litigation associated with health screenings and remote work. Courts have yet to decide on BIPA's extraterritorial application and statute of limitations, the resolution of which could impact the viability of a number of BIPA cases.

Standing in Federal Court. As set out in last year's Review, there has been a flood of class actions against large corporations following the Illinois Supreme Court's decision in *Rosenbach v. Six Flags*, which conferred standing on plaintiffs who allege BIPA violations even without pleading an actual injury.[373] In 2020, the Seventh Circuit took a similar position in *Bryant v. Compass Group USA, Inc*., holding that a procedural violation of section 15(b) of BIPA is sufficient to constitute an injury for Article III standing.[374] Subsequently, in *Fox v. Dakkota Integrated Systems*, the Seventh Circuit held that federal courts can also hear claims under section 15(a) of BIPA when plaintiffs allege a "concrete and particularized harm," such as an invasion of the privacy interest in biometric data.[375]

BIPA Settlements. The trend of sizeable settlements that we noted in last year's Review has persisted throughout 2020, including a BIPA class action suit involving a large social media company that settled for $650 million in August 2020.[376] Given the law's mandatory statutory penalties of $1,000 per negligent violation or $5,000 per intentional or reckless violation, even this settlement may represent only a small percentage of the possible statutory damages.[377] The decisions affirming plaintiffs' standing to bring BIPA suits in at least some federal courts[378] and the large settlements at issue, indicate we will likely continue to see significant BIPA litigation in 2021.

Compelling Arbitration in Employment-Related BIPA Lawsuits. Lawsuits against employers that collect employees' biometric data for timekeeping purposes continue to represent a significant portion of BIPA cases in state and federal courts.[379] In last year's Review, we reported that some plaintiff-employees had successfully used BIPA to avoid being compelled into arbitration.[380] Although some plaintiffs achieved similar results in 2020,[381] other plaintiffs were indeed compelled into arbitration based on the courts' analysis of the arbitration agreements at issue.[382]

BIPA Preemption by State Laws. Another 2020 development in employee-related BIPA litigation was an Illinois court decision holding that employees may pursue BIPA claims without preemption by the Illinois Workers' Compensation Act, which is generally read to be an exclusive remedy for workplace injuries.[383] At the same time, however, courts continue to hold that BIPA is preempted by the Labor Management Relations Act[384] and Railway Labor Act.[385]

Extraterritorial Application of BIPA. On this point, in 2020 some employees attempted to bring BIPA claims not only against in-state employers but also against third-party operators of workplace systems that collect biometric data, even if not based in Illinois.[386] These and other suits against out-of-state companies have implicated questions about the extraterritorial scope of BIPA. In a recent case involving an insurer, the Illinois Supreme Court held that a statute can be applied extraterritorially even without "clear intent" in its statutory language if "the circumstances that relate to the disputed transaction occur primarily and substantially in Illinois."[387] But the extent to which, under this holding, events must take place in Illinois for BIPA to apply to out-of-state entities remains an open question.

COVID-19-Related BIPA Litigation. The COVID-19 pandemic has also created additional BIPA litigation. Employees have alleged that certain COVID-19 safety protocols imposed by employers collect biometric information in violation of BIPA.[388] Parents have also brought lawsuits on behalf of their children using educational platforms for remote learning that allegedly collect and store biometric data in violation of BIPA.[389] We anticipate that more COVID-19-related BIPA litigation is likely to take place as workplaces and educational institutions impose screening measures on workers and students for identification remotely.

Statute of Limitations. The statute of limitations for BIPA remains unsettled, as the law contains no express provision establishing a statute of limitations. While a few state and federal courts have found that there is a five-year statute of limitations period for BIPA,[390] this question is currently pending in the Illinois First Appellate District in *Tims v. Black Horse Carriers, Inc*.[391] The *Tims* decision could have a substantial impact on the viability of future BIPA lawsuits, particularly if the court rules in favor of the defendants and holds that BIPA's statute of limitations period is only one year.

F. Other Notable Cases

In addition to the cases described above, 2020 has seen important updates on cases previously reported in last year's Review, as well as new matters concerning children's privacy and remote learning, connected vehicles and devices, and new legal questions in the fintech space.

Technology Company – Location History. A technology company has been accused of withholding relevant information in connection with the proposed class action alleging the company illegally tracked and stored users' location data.[392] The plaintiffs have moved to lift the stay on discovery requested by the technology company after they filed an amended complaint based on evidence surfaced by contemporaneous litigation brought by the Arizona Attorney General's Office.[393] The court has yet to rule on the motion.[394]

Technology Company – Medical Records. In September, U.S. District Court for the Northern District of Illinois granted the motion to dismiss all claims in a suit concerning the release of depersonalized medical information by a university to a technology company as part of a research partnership.[395] The proposed class action had alleged that the technology company and the university engaged in deceptive business practices for turning over medical information on all patients who were treated at the university's medical center from 2009 through 2016.[396] The court found that the plaintiff had not sufficiently alleged any harm as a result of this practice, and thus dismissed all claims. The plaintiff stated plans to appeal this decision.[397]

Connected Vehicles and Devices and the Internet of Things. Likewise, in March 2020, the U.S. District Court for the Southern District of Illinois dismissed a case against an automobile manufacturer alleging that defects in vehicle infotainment systems had left them vulnerable to hacking.[398] The court reasoned that the threat of future harm from such potential hacking did not constitute a sufficiently cognizable injury to give standing to the plaintiffs, who alleged that the vulnerabilities substantially undermined the value of the vehicles compared to what they had paid.[399] The plaintiffs have since appealed the decision to the United States Court of Appeals for the Seventh Circuit, arguing that the

lower court did not properly consider the evidence of the vulnerabilities and the valuation decrease as a result.[400]

The Wiretap Act and Technology Companies. Additional connected-devices cases continue to work their way through the federal courts, raising both state and federal claims.[401] A case in the U.S. District Court for the District of New Jersey against electronics companies for harvesting data from "smart TVs," which partially survived a motion to dismiss in 2019, has again survived dismissal of the amended complaint alleging federal Wiretap Act violations.[402] In its second order, the court restated its previous conclusion that the electronics companies do not constitute "parties" to the communications at issue (which could have exempted them from liability); rather, the court found them analogous to smartphone companies, entities that have been held to be "hosts," not participants, and thus subject to the Wiretap Act.[403] The court also rejected an interlocutory appeal, finding that there were still factual issues to be resolved.[404] The electronics companies have now moved for a separation of the claims, arguing that moving forward in discovery as joint defendants with a rival company would materially harm their business interests.[405] The companies have also filed a motion to compel individual arbitration and strike the class claims. The court granted a motion to sever the claims, but has yet to rule on whether to compel arbitration.[406]

COPPA and Child Privacy Cases. Virtual learning and a renewed focus on children's privacy during the pandemic have resulted in a new wave of litigation related to the collection of data from children, including under the Children's Online Privacy Protection Rule promulgated under COPPA.[407] The State of New Mexico brought claims in federal court against a major technology company for collecting data from children using its free classroom services and computers provided to underserved communities for online learning.[408] The lawsuit alleged that the company used these free services to track the online activities of students without proper notice to or consent from the students or their parents.[409] Although the case was dismissed for insufficiently alleging a violation of COPPA because of disclosures on the company's website about the services and data collection practices, the New Mexico Attorney General has appealed the dismissal, the resolution of which is still pending.[410]

The privacy of minors in online and mobile device gaming has also continued to make headlines. As we covered in last year's Review, a class action against gaming and app creation companies in California survived a critical motion to dismiss in 2019.[411] The plaintiffs brought a proposed class action against these companies for allegedly selling information gathered from games aimed at children and adolescents without parental consent.[412] On August 5, 2020, the parties agreed to settle out of court. The proposed settlements do not include any monetary award for class members, but would limit the companies' ability to collect information from children using their apps.[413] More recently, the FTC filed a complaint against a popular gaming app developer, alleging the company allowed third-party ad networks to collect information by tracking user behavior from child-directed apps without proper notice to or consent from the parents.[414] The action is pending in federal court.

Similarly, a video streaming company settled a case with the New York Attorney General and the FTC involving allegations of COPPA violations for tracking and targeting advertisements to users watching videos directed at children under 13 for a record $170 million.[415] Although this case has been settled, similar allegations have been raised in the UK in a suit alleging damages of over $2 billion.[416]

Fintech Litigation. Financial technology (fintech) companies have also increasingly become the target of privacy concerns for their collection of both personal banking data and transaction-level data from users. On August 25, 2020, users of a fintech service brought a proposed class action in the U.S. District Court for the Northern District of California against a fintech company, alleging that the company mishandles sensitive user information. The plaintiffs claim that the company, which provides budgeting tools, savings trackers, account history information and account verification, invades the privacy of users by collecting transaction-level data without the knowledge or consent of its users, and puts that sensitive information at risk by sending these consumer files to third-party buyers in an easily hackable format.[417] On November 4, 2020, the company filed a motion to dismiss the proposed class action suit for failure to state a claim, arguing that the company collects and sells the consumer data only after it has been anonymized and aggregated with the anonymized data of other consumers; therefore, consumers can have no reasonable expectation of privacy in it.[418] The court has yet to rule on this motion.[419]

On May 4, 2020, another fintech company whose product is utilized by banking and financial apps was accused of accessing, using, and selling app customers' personal banking data without their consent, according to a proposed class action (also filed in the Northern District of California).[420] The parties are awaiting a decision on the company's motion to dismiss.

III. GOVERNMENT DATA COLLECTION

A. Collection of Cell Phone Data

In 2020, a number of cases addressed the issue of individuals' privacy rights with respect to digital data stored on cell phones and similar personal electronic devices. Several court decisions strengthened the government's ability to collect and search data without warrants through the Fourth Amendment's "third-party" doctrine, under which a person generally "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[421] However, courts have reached divergent conclusions regarding the government's ability to collect digital data under the Foreign Intelligence Surveillance Act (FISA).

Cases Regarding the Collection of Personal Data. In June 2020, the U.S. Court of Appeals for the Fifth Circuit held that an individual does not have a Fourth Amendment privacy interest in the records of their Bitcoin transactions.[422] The court declined to extend the limitation of the third-party doctrine as it applies to cell phones to either Bitcoin's public blockchain or to records from a virtual currency exchange.[423] The court analogized Bitcoin blockchain and the virtual currency exchange's records to bank records and telephone call logs because: (1) they contain limited information; and (2) transferring and receiving Bitcoin requires an affirmative act, which is more akin to voluntarily placing a call than an unknowing collection of cell phone location data.[424] The court also noted that Bitcoin users are unlikely to expect that the Bitcoin transaction data will be kept private since every transaction is recorded in a publicly available blockchain.[425]

In *United States v. Carme*, a Barnstable police detective used BitTorrent-deciphering software to download 192 public files, which helped generate evidence against a criminal defendant.[426] When

this tactic was challenged on Fourth Amendment grounds, the district court for the District of Massachusetts declined to expand privacy protections to file-sharing software that makes it harder for third parties to view the entirety of a file (unlike traditional peer-to-peer file-sharing, which makes such viewing *easier*).[427] In reaching this result, the court stressed that there is no reasonable expectation of privacy when a matter is voluntarily disclosed or entrusted to third parties, even if the particular file-sharing software gave the illusion of additional privacy by fragmenting the contents of shared files.[428]

In *United States v. Trader*, the Eleventh Circuit Court of Appeals similarly found that the government's warrantless collection of a criminal suspect's email address and internet protocol addresses from a third party's business records was constitutional and did not violate the Fourth Amendment.[429] The *Trader* court emphasized that a business record that might incidentally reveal location information, such as an email address or internet protocol address, falls outside the narrow exception to the third-party doctrine as it applies to cell phone location records.[430]

Data Collection Pursuant to a FISA Order. In another notable development, this past year saw the federal courts further divide on when and under what conditions the government's data collection under FISA might violate the Fourth Amendment.

On September 2, 2020, the Ninth Circuit ruled that the National Security Agency (NSA) violated Section 1861 of FISA by collecting phone records in bulk without showing their relevance to any specific, authorized, and existing investigation before collection.[431] The NSA collected from major telecommunication providers call records or telephony metadata for communications: (1) between the United States and abroad; and (2) wholly within the United States, including the defendant's local phone calls.[432] These records included information such as the phone numbers involved in a call and the time and duration of the call, but not the voice content of any call.[433] The Ninth Circuit distinguished the data at issue from *Smith v. Maryland*,[434] a Supreme Court case that involved the government installing a "pen register," a device that records numbers dialed from a phone.[435] Instead, analogizing the data at issue in this case to the cell phone location information in *Carpenter v. United States*,[436] the court found that an individual's telephony metadata collected on a continuing basis is akin to 24-hour surveillance.[437] The Ninth Circuit did not, however, reach an ultimate conclusion on whether the government's metadata collection program was therefore prohibited by the Fourth Amendment.

In a December 2019 decision, however, the U.S. Court of Appeals for the Second Circuit reached a contrasting result when applying the Fourth Amendment to email collection under FISA.[438] The court in that case, *United States v. Hasbajrami*, found the "incidental collection" of communications—the collection of the communications of individuals in the United States acquired in the course of the surveillance of individuals without ties to the United States and located abroad—was permissible under the Fourth Amendment.[439] The court noted that surveillance in *Hasbajrami* was permissible under Section 702 of FISA, and that the government does not have to return to the FISA court to seek approval before it undertakes surveillance of any specific individual.[440]

FISA Authorities Lapsed. As mentioned briefly above, in March 2020, three FISA authorities lapsed[441]: (1) Section 215 of the USA Patriot Act, also known as the "business records" provision;[442] (2) the "lone wolf" authority;[443] and (3) the "roving wiretap" authority.[444] Each

has, in the past, been a prominent law enforcement tool. Under Section 215, the NSA can petition the Foreign Intelligence Surveillance Court (FISC) to order the production of business records and other tangible things relevant to specific investigations.[445] The lone wolf authority allows the FBI to surveil a non-U.S. citizen who is suspected of planning a terrorist attack but cannot be linked to a foreign terrorist organization.[446] Finally, the roving wiretap authority enables the FBI to continue the wiretap of a criminal suspect, even if the suspect switches phones.[447] It is meant for individuals using burner phones or alternating between several devices.[448] To date, as set out at Section I.C.2., these sources of authority have not been reauthorized, setting the stage for further legislative action in 2021.

B. Extraterritorial Warrants and Data Transfers

In 2018, Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).[449] A year later, the United Kingdom passed a similar law called the Crime (Overseas Production Orders) Act 2019.[450] Based on these mirroring statutes, the United States and the United Kingdom entered into the first-ever CLOUD Act bilateral pact: the US-UK Bilateral Data Access Agreement, known as "DICA" in 2019.[451] The Agreement came into force on July 8, 2020.[452]

While the United States had engaged in negotiations with Australia[453] and the European Union[454] to implement similar bilateral pacts in 2019, no agreement has been finalized. Nevertheless, Australia took several steps in 2020 suggesting an agreement may be close. In spring 2020, the Australian government introduced legislation that would provide the legal basis, where a designated international agreement is in place, for sending data requests directly to foreign providers, explicitly noting that "[t]he Bill provides the legislative framework for Australia to give effect to future bilateral and multilateral agreements for cross-border access to electronic information and communications data."[455] The Australian Parliamentary Joint Committee on Intelligence and Security also issued a call for public comments concerning the legislation.[456] Many businesses and organizations responded with comments reflecting broader critiques of the CLOUD Act—such as the Australian Privacy Foundation's statement that the bill is "deeply flawed."[457] That said, although no additional CLOUD Act formal agreements were made in 2020, additional bilateral agreements may still be finalized in 2021.

There may be, however, a significant complicating factor for any EU-US bilateral agreement. On July 16, 2020, the Court of Justice of the European Union (CJEU) struck down the U.S.-EU Privacy Shield as legally invalid (*Schrems II*).[458] CJEU noted that, under the EU's General Data Protection Regulation (GDPR), a transfer of personal data out of the EU may take place only if the third country ensures an adequate level of data protection. Maximilian Schrems, a resident of Austria, lodged a series of complaints with the Irish supervisory authority, the Data Protection Commission (DPC), seeking to prohibit the transfer of his personal data from the European subsidiary of a social media company to its parent corporation in the U.S.[459] In deciding Schrems's case, CJEU found that limitations on the protection of personal data in the U.S. meant that country's domestic law failed to meet EU requirements. Specifically, CJEU found that: (1) U.S. law does not adequately limit the personal data that U.S. public authorities may access and use through surveillance programs; and (2) the relevant provisions in U.S. law do not grant data subjects actionable rights before the courts as against U.S. governmental authorities.[460]

On August 10, 2020, the U.S. Department of Commerce and the European Commission announced, in response to the *Schrems II* decision, that they had initiated discussions to evaluate the potential for an enhanced U.S.-EU Privacy Shield framework to comply with the CJEU's *Schrems II* ruling.[461] That same month, a European privacy group filed a lawsuit against over 100 websites, alleging the sites were still sending data to the United States in violation of the CJEU's decision.[462]

C. Other Notable Developments

1. Police Use of Facial Recognition Software

Facial recognition software (FRS) gained publicity in 2020 not only for its potential use in controlling the spread of COVID-19,[463] but also for its widespread adoption by federal and local law enforcement. The technology's accuracy has been called into question by an MIT study, which found that FRS results in a disproportionate number of misidentifications, particularly for individuals of color.[464] Tensions heightened after media reports revealed that several law enforcement agencies had contracted with an FRS company that had scraped over three billion images from publicly available social media websites without consent.[465] These reports gave rise to greater scrutiny, including a March 2020 action brought by the Vermont Attorney General[466] and a May 2020 action by the ACLU alleging violations of Illinois's Biometric Information Privacy Act (BIPA).[467]

Cities and local governments have begun responding to this backlash. For example, the New York Police Department (NYPD) published protocols limiting its own use of facial recognition.[468] This updated policy requires that facial recognition technology only be used for legitimate law enforcement purposes, and that a facial recognition match may serve as a lead but does not constitute probable cause for an arrest.[469] Similarly, the Los Angeles Police Department (LAPD) has barred officers and detectives from using third-party facial recognition platforms in their investigations.[470] And as discussed at Section I.C.1., various municipalities have either banned or significantly curtailed the use of FRS.

2. Government Use of Aerial Surveillance

In a further development at the intersection of privacy and law enforcement, in recent years the Baltimore Police Department (BPD) launched its controversial "Aerial Investigation Research," or "AIR," program. Three aircraft equipped with high-definition cameras now fly above Baltimore for 12 hours each day to identify specific individuals who are suspected of committing or witnessing serious crimes, as well as those who crossed their paths before and after the crimes took place.[471] On April 9, 2020, community activists and city residents brought a 42 U.S.C. § 1983 action against the BPD, alleging this aerial surveillance violated their First Amendment associational rights and Fourth Amendment protection against unreasonable searches.[472] The district court denied the plaintiffs' request for a preliminary injunction against the BPD program, likening it to conventional surveillance techniques the Supreme Court found to be permissible in *Carpenter v. United States*.[473]

On appeal, a panel of the Fourth Circuit upheld the program as constitutional, in part because the AIR cameras do not photograph a person's features, but rather reduce each individual on the ground to a pixelated dot.[474] The court also noted that BPD officers can only access these photographs if specific violent crimes are reported in a particular location, and cannot identify someone photographed by AIR

without relying on ground-based cameras.[475] The court also held the program does not violate a reasonable expectation of privacy because an individual has a limited expectation of privacy in public, and AIR only constitutes *short-term* surveillance of an individual's public movements.[476] Finally, the court found that the program does not violate First Amendment rights to freely associate because individuals would not likely be deterred from associating simply to avoid showing up as dots in surveillance photographs.[477] However, an *en banc* rehearing request was granted by the full Fourth Circuit in December 2020, leaving the question far from settled.

3. Scooter Companies Required to Share Real-Time Location Data

Also this past year, the Los Angeles Department of Transportation (LADOT) renewed its One Year Dockless Mobility permit program for the operation of scooter ride-sharing businesses in Los Angeles. The program offers businesses a permit is contingent on such businesses sharing real-time location data with the city.[478] In March, the scooter ride-sharing subsidiary of a large ride-sharing business sued the LADOT over this data-sharing requirement, arguing that in practice, the rule operates as a warrantless administrative search. On this point, the scooter ride-sharing subsidy claimed that LADOT or others can use the time-stamped geolocation data to identify individual users' travel patterns.[479] The case was voluntarily dismissed without prejudice by the scooter-riding subsidiary on June 15, 2020 after that entity was acquired by a different scooter ride-sharing company.[480] In June, however, the ACLU filed a complaint on behalf of the scooter ride-share users raising similar privacy arguments.[481] Of note, the LADOT's scooter requirements underscore a limit in CCPA protections: because the location data is provided to the government and not for a commercial purpose, that law would not apply.

IV. CONCLUSION

2020 was, in every sense of the word, unprecedented. U.S. privacy and cybersecurity law and policy have been forced to evolve at a breakneck pace, both to face long-standing risks (like sophisticated, state-sponsored cybercriminals) and once-in-a-generation challenges (like a worldwide pandemic). These changes will reverberate throughout 2021 and beyond, shaping how companies, governments, and the general public use, protect, and regulate data. In the year ahead, we will continue to track these important issues.

---

[1] *See* Gretchen Ramos and Darren Abernathy, *Additional U.S. States Advance the State Privacy Legislation Trend in 2020*, National Law Review (Dec. 15, 2020), *available at* https://www.natlawreview.com/article/additional-us-states-advance-state-privacy-legislation-trend-2020.

[2] 2020 Democratic Party Platform (Aug. 18, 2020), *available at* https://www.demconvention.com/wp-content/uploads/2020/08/2020-07-31-Democratic-Party-Platform-For-Distribution.pdf.

[3] *Id.*

[4] Press Release, Department of Justice, *The Justice Department Unveils Proposed Section 230 Legislation* (Sept. 23, 2020), *available at* https://www.justice.gov/opa/pr/justice-department-unveils-proposed-section-230-legislation; Department of Justice's Review of Section 230 of the Communications Decency Act of 1996, *available at* https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996.

[5] Press Release, State of California Department of Justice, *Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit* (July 19, 2012), *available at* https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.

[6] *See* Reuters Staff, *U.S. FTC chair says he will resign along with senior staff*, Reuters (Jan. 19, 2021), *available at* https://www.reuters.com/article/us-ftc-simons/us-ftc-chair-says-he-will-resign-along-with-senior-staff-idUSKBN29O1XB.

[7] Michelle Price, *Biden appoints U.S. consumer watchdog veteran as acting director after Trump appointee resigns*, Reuters (Jan. 21, 2021), *available at* https://www.reuters.com/article/us-usa-biden-cfpb/biden-appoints-u-s-consumer-watchdog-veteran-as-acting-director-after-trump-appointee-resigns-idUSKBN29Q249.

[8] President Biden's late son, Beau Biden, served as attorney general of Delaware, and Harris served as attorney general of California.

[9] Michelle Price, *Biden appoints U.S. consumer watchdog veteran as acting director after Trump appointee resigns*, Reuters (Jan. 21, 2021), *available at* https://www.reuters.com/article/us-usa-biden-cfpb/biden-appoints-u-s-consumer-watchdog-veteran-as-acting-director-after-trump-appointee-resigns-idUSKBN29Q249.

[10] H.R. 748, CARES Act, Public Law 116-136 (Mar. 27, 2020).

[11] *See* Stephen Carroll, *Biden begins political battle for $1.9 trillion stimulus plan*, France24 (Jan. 21, 2021), *available at* https://www.france24.com/en/tv-shows/business-daily/20210121-president-biden-begins-political-battle-for-1-9-trillion-stimulus-plan.

[12] *See* Eleanor Laise, *Joe Biden Could Face an Uphill Battle to Restore Consumer Protections*, Barron's (Nov. 13, 2020), *available at* https://www.barrons.com/articles/whats-next-for-the-cfpb-and-why-it-matters-51605307530.

[13] Lesley Fair, *Operation Corrupt Collector cracks down on illegal debt collection tactics*, Federal Trade Commission (Sept. 29, 2020), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2020/09/operation-corrupt-collector-cracks-down-illegal-debt.

[14] S. 3663, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3663/text.

[15] *Id*.

[16] Allison Grande, *Sens. Float Privacy Bill To Protect Data In COVID-19 Era*, Law 360 (Apr. 30, 2020) *available at* https://www.law360.com/articles/1269228/sens-float-privacy-bill-to-protect-data-in-covid-19-era; Adam Schwartz, *Two Federal COVID-19 Privacy Bills: A Good Start and a Misstep*, Electronic Frontier Foundation (May, 28, 2020), *available at* https://www.eff.org/deeplinks/2020/05/two-federal-covid-19-privacy-bills-good-start-and-misstep.

[17] S. 3749, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3749/text.

[18] *Id*.

[19] U.S. Department of Health & Human Services, *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* (Mar. 30, 2020), *available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

[20] U.S. Department of Health & Human Services, *OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency* (Apr. 2, 2020), *available at* https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html; U.S. Department of Health & Human Services, *OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency* (Apr. 9, 2020), *available at* https://web.archive.org/web/20210117020355/ https://www.hhs.gov/about/news/2020/04/09/ocr-announces-notification-enforcement-discretion-community-based-testing-sites-during-covid-19.html.

[21] U.S. Department of Health & Human Services, *OCR Issues Guidance to Help Ensure First Responders and Others Receive Protected Health Information about Individuals Exposed to COVID-19* (Mar. 24, 2020), *available at* https://web.archive.org/web/20210117001045/ https://www.hhs.gov/about/news/2020/03/24/ocr-issues-guidance-to-help-ensure-first-responders-and-others-receive-protected-health-information-about-individuals-exposed-to-covid-19.html.

[22] U.S. Department of Health & Human Services, *OCR Issues Guidance on How Health Care Providers Can Contact Former COVID-19 Patients About Blood and Plasma Donation Opportunities* (June 12, 2020), *available at* https://web.archive.org/web/20210116081727/ https://www.hhs.gov/about/news/2020/06/12/guidance-on-hipaa-and-contacting-former-covid-19-patients-about-blood-and-plasma-donation.html.

[23] Centers for Disease Control and Prevention (CDC), *COVID-19 Vaccination Program Interim Playbook for Jurisdiction Operations* (Oct. 29, 2020) *available at* https://www.cdc.gov/vaccines/imz-managers/downloads/COVID-19-Vaccination-Program-Interim_Playbook.pdf.

[24] Sheryl Gay Stolberg, *Some States Balk After C.D.C. Asks for Personal Data of Those Vaccinated*, N.Y. Times (Dec. 8, 2020) *available at* https://www.nytimes.com/2020/12/08/us/politics/cdc-vaccine-data-privacy.html.

[25] Act in relation to the collection of emergency health data and personal information and the use of technology to aid during COVID-19; and providing for the repeal of such provision upon the expiration thereof, S.8848D (N.Y. 2020), *available at* https://legislation.nysenate.gov/pdf/bills/2019/S8448D.

[26] Cal. Civ. Code §§ 1798.130(a)(5)(D), 1798.146, and 1798.148.

[27] Act to amend Section 1798.130 of, and to add Sections 1798.146 and 1798.148 to, the Civil Code, relating to consumer privacy, and declaring the urgency thereof, to take effect immediately, A.B. 713 (Cal. 2020) (enacted), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB713.

[28] Cal. Civ. Code §§ 1798.130(a)(5)(D), 1798.146, and 1798.148.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] Act concerning governmental response to the 2020 COVID-19 pandemic in Kansas, H.B. 2016 (Kan. 2020) (enacted), *available at* http://www.kslegislature.org/li_2020s/b2020s/measures/documents/hb2016_enrolled.pdf.

[33] N.Y. Pub. Health Code § 2181 Act to amend the public health law, in relation to the confidentiality of contact tracing information, S.8450C (N.Y. 2020), *available at* https://legislation.nysenate.gov/pdf/bills/2019/S8450C.

[34] Act relating to contact tracing of the COVID-19 virus, S.B.1 (Ala. 2020), *available at* http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2021RS/PrintFiles/SB1-int.pdf.

[35] *Id.*

[36] Act concerning data privacy related to certain health information and supplementing Title 26 of the Revised Statutes, A.4170 (N.J. 2020), *available at* https://www.njleg.state.nj.us/2020/Bills/A4500/4170_R1.HTM.

[37] *Id.*

[38] *Id.*

[39] An act to amend the general business law, in relation to the management and oversight of personal data [the "New York Privacy Act"], S. 5642, 2019-2020 Leg., Reg. Sess. (N.Y. 2019), *available at* https://legislation.nysenate.gov/pdf/bills/2019/S5642.

[40] An act to amend the general business law and the state technology law, in relation to notification of a security breach, S5575B, 2019-2020 Leg., Reg. Sess. (N.Y. 2019), *available at* https://www.nysenate.gov/legislation/bills/2019/s5575/amendment/b

[41] Act in relation to the collection of emergency health data and personal information and the use of technology to aid during COVID-19; and providing for the repeal of such provision upon the expiration thereof, S.8848D (N.Y. 2020), *available at* https://www.nysenate.gov/legislation/bills/2019/S8448.

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *See* Act in relation to the collection of emergency health data and personal information and the use of technology to aid during COVID-19; and providing for the repeal of such provision upon the expiration thereof, S.301 (N.Y. 2021), *available at* https://www.nysenate.gov/legislation/bills/2021/S301; Act in relation to the collection of emergency health data and personal information and the use of technology to aid during COVID-19; and providing for the repeal of such provision upon the expiration thereof, H.687 (N.Y. 2021), *available at* https://legislation.nysenate.gov/pdf/bills/2021/A687.

[46] Act to add Title 1.81.10 (commencing with Section 1798.600) to Part 4 of Division 3 of the Civil Code, relating to personal information, A.B.660 (Cal. 2020), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB660.

[47] *Id.*

[48] Act to add Title 4.5 (commencing with Section 1924) to Part 4 of Division 3 of the Civil Code, to add Chapter 5 (commencing with Section 104000) to Part 2 of Division 102 of the Health and Safety Code, and to add Part 6 (commencing with Section 22360) to Division 2 of the Public Contract Code, relating to personal information, A.B.1782 (Cal. 2020), *available at* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1782.

[49] *Id.*

[50] *Id.*

[51] Bill for an act relating to health, H.F.164 (Minn. 2020), *available at* https://www.revisor.mn.gov/bills/text.php?number=HF164&type=bill&version=0&session=ls91&session_year=2020&session_number=1.

[52] *See* Act to Exempt EMS telecommunicator info from Public Records Law, S.B. 31 (Ohio 2020), *available at* https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA133-SB-31.

[53] *See* Press Release, Office of the Attorney General, *Attorney General Herring Tells Tech Companies to Protect Public from Shady "Contact Tracing Apps"* (June 17, 2020), *available at* https://www.oag.state.va.us/media-center/news-releases/1739-june-17-2020-herring-tells-tech-companies-to-protect-public-from-shady-contact-tracing-apps.

[54] *Id.*

[55] *See* Press Release, N.Y. State Office of the Attorney General, *Attorney General James Secures New Protections, Security Safeguards for All Zoom Users* (May 7, 2020), *available at* https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users.

[56] *Id.*

[57] *See* Cal. Civ. Code § 1798.140(c).

[58] *See, e.g.*, *California Approves Final CCPA Regulations, and Bill Extending Key Exemptions Moves Forward at the Legislature*, Gibson Dunn (Aug. 20, 2020), *available at* https://www.gibsondunn.com/california-approves-final-ccpa-regulations-and-bill-extending-key-exemptions-moves-forward-at-the-legislature/; *California Consumer Privacy Act Update: Attorney General Finalizes Regulations and Provides Interpretive Guidance*, Gibson Dunn (June 12, 2020), *available at* https://www.gibsondunn.com/california-consumer-privacy-act-update-attorney-general-finalizes-regulations-and-provides-interpretive-guidance/; *California Consumer Privacy Act Update: Attorney General Proposes Further Revisions to CCPA Regulations*, Gibson Dunn (Mar. 17, 2020), *available at* https://www.gibsondunn.com/california-consumer-privacy-act-update-attorney-general-proposes-further-revisions-to-ccpa-regulations/; *California Consumer Privacy Act Update: Attorney General Proposes Regulations Version 2.0*, Gibson Dunn (Feb. 19, 2020), *available at* https://www.gibsondunn.com/california-consumer-privacy-act-update-attorney-general-proposes-regulations-version-2-0/.

[59] *Final Text of Proposed Regulations*, State Cal. Dep't Just. Off. Att'y Gen. (Jan. 19, 2020), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf?

[60] *Id.*

[61] *Text of Fourth Set of Proposed Modifications*, State Cal. Dep't Just. Off. Att'y Gen. (Dec. 10, 2020), *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-prop-mods-text-

of-regs-4th.pdf; *Text of Third Set of Proposed Modifications – Comparison Version*, State Cal. Dep't Just. Off. Att'y Gen. (Oct. 12, 2020), *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf?.

[62] *Text of Fourth Set of Proposed Modifications*, State Cal. Dep't Just. Off. Att'y Gen. (Dec. 10, 2020), *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-prop-mods-text-of-regs-4th.pdf; *Text of Third Set of Proposed Modifications – Comparison Version*, State Cal. Dep't Just. Off. Att'y Gen. (Oct. 12, 2020), *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf?.

[63] *See, e.g.*, *The Potential Impact of the Upcoming Voter Initiative, the California Privacy Rights Act*, Gibson Dunn (Sept. 29, 2020), *available at* https://www.gibsondunn.com/potential-impact-of-the-upcoming-voter-initiative-the-california-privacy-rights-act/; *As California Consumer Privacy Act Enforcement Commences, a Tougher New Data Privacy Law Will Go Before California Votes in November*, Gibson Dunn (July 1, 2020), *available at* https://www.gibsondunn.com/as-california-consumer-privacy-act-enforcement-commences-a-tougher-new-data-privacy-law-will-go-before-california-voters-in-november/.

[64] Whereas the CCPA defines "business" in part as a for-profit entity that collects consumers' personal information, which does business in California and possesses "the personal information of 50,000 or more consumers, households, or devices," Cal. Civ. Code § 1798.140(c)(1)(B) [prior CCPA text], the CPRA will remove such devices from consideration. *See* Cal. Civ. Code § 1798.140(d)(1) [as modified by CPRA].

[65] *Compare* Cal. Civ. Code § 1798.140(c)(1)(B) [prior CCPA text], *with* Cal. Civ. Code § 1798.140(d)(1)(B) [as modified by CPRA].

[66] *Compare* Cal. Civ. Code § 1798.140(c)(1)(C) [prior CCPA text], *with* Cal. Civ. Code § 1798.140(d)(1)(C) [as modified by CPRA].

[67] *Compare* Cal. Civ. Code § 1798.140(o)(2) [prior CCPA text] *with* Cal. Civ. Code § 1798.140(v)(2) [as modified by CPFRA].

[68] *Compare* Cal. Civ. Code § 1798.140(t) [prior CCPA text], *with* Cal. Civ. Code § 1798.140(ad) [as modified by CPRA].

[69] An Act to Protect the Privacy of Online Customer Information, S. P. 275, 2019 Leg., 129th Sess. (Me. 2019), *available at* http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=9&snum=129.

[70] *Id.*

[71] *Id.*

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

[73] An Act relating to public safety; designating the month of October of each year as "Cybersecurity Awareness Month"; revising requirements relating to emergency response plans for schools, cities, counties and resort hotels; clarifying the authority of the Governor to call members of the Nevada National Guard into state active duty upon a request for assistance from certain governmental entities that have experienced a significant cybersecurity incident; requiring each city or county to adopt and maintain a cybersecurity incident response plan; revising the duties of the Nevada Office of Cyber Defense Coordination of the Department of Public Safety; requiring the Office to submit a quarterly report to the Governor regarding cybersecurity; revising provisions relating to the disclosure of records by the Office; and providing other matters properly relating thereto, S.B. 69, 2019 Leg., 80th Sess. (Nev. 2019), *available at* https://www.leg.state.nv.us/Statutes/80th2019/Stats201915.html#Stats201915_CH412.

[74] *Id.*

[75] *Id.*

[76] An act to amend the general business law and the state technology law, in relation to notification of a security breach, S5575B, 2019-2020 Leg., Reg. Sess. (N.Y. 2019), *available at* https://www.nysenate.gov/legislation/bills/2019/s5575/amendment/b.

[77] *Id.*

[78] Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019-2020 Leg., Reg. Sess. S5575B (N.Y. 2019), *available at* https://legislation.nysenate.gov/pdf/bills/2019/S5575B.

[79] *See id.* § 899-BB(1)(a).

[80] *Id.*

[81] N.Y. Bar Ass'n, *January 21, 2021 State Legislative Developments*, NYBA Online (Jan. 22, 2021), *available at* https://www.nyba.com/NYBA/Publications/Friday_s_News/NYBA/Publications/Fridays_News.aspx?hkey=79bbbf02-4315-4d19-8349-fe28b3a3de2e.

[82] NYDAT § 899-CC(7).

[83] An act to amend the general business law, in relation to the management and oversight of personal data [the "New York Privacy Act"], S. 5642, 2019-2020 Leg., Reg. Sess. (N.Y. 2019), *available at* https://legislation.nysenate.gov/pdf/bills/2019/S5642.

[84] *Id.*

[85] *See* Josefa Velasquez, *New York's State Senate Democrats Gain a Supermajority. What Could They Do With It?*, The City (Nov. 23, 2020), *available at* https://www.thecity.nyc/2020/11/23/21612024/new-york-state-senate-democrats-gain-a-supermajority.

[86] An Act Relating to actions with respect to a breach of security that involves personal information, S.B. 684, 80th Or. Leg. Assemb., Reg. Sess. (O.r. 2019), *available at* https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/SB684/Enrolled.

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] An Act Relating to security measures required for devices that connect to the Internet, H.B. 2395, 80th Leg. Assemb., Reg. Sess. (Or. 2019), *available at* https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled.

[93] *Id.*; An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy, S.B. 327, 2017-2018 Leg., Reg. Sess. (Cal. 2018), *available at* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327.

[94] An Act Relating to the use of facial recognition services, S.B. 6280, 66th Leg., Reg. Sess. (Wash. 2020), *available at* http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Session%20Laws/Senate/6280-S.SL.pdf?q=20201214093740.

[95] *Id.*

[96] *Id.*

[97] For the bill's current language, as submitted to the Washington State Legislature, *see* Wash. State Leg. Committee Schedule, Bill Req. S-4873.3/20 3rd draft ["Concerning the management and oversight of personal data"], *available at* https://app.leg.wa.gov/committeeschedules/Home/Document/208507; for the draft version bearing Senator Carlyle's name, see @Reuvencarlyle, Twitter (Sept. 9, 2020), *available at* https://twitter.com/Reuvencarlyle/status/1303808769218945025.

[98] Reuven Carlyle, *Washington Privacy Act 2021 (DRAFT)*, Senate Democrats (Aug. 5, 2020).

[99] *Id.*

[100] An Act relating to privacy, H.B. 2572, 30th Leg., Reg. Sess. (Haw. 2020), *available at* https://www.capitol.hawaii.gov/session2020/bills/HB2572_SD1_.pdf; An Act relative to consumer data privacy, Bill S.120, 191st General Court (Mass. 2019), *available at* https://malegislature.gov/Bills/191/S120/BillHistory; An Act relating to biological characteristics, H.B. 2478, 44th Leg., 1st Reg. Sess.(Ariz. 2019), *available at* https://www.azleg.gov/legtext/54leg/1R/bills/HB2478P.pdf.

[101] Henry Kenyon, *Voters in Portland, Maine, vote to ban use of facial recognition tech*, CQ Roll Call Washington Data Privacy Briefing (Nov. 6, 2020), *available at* https://today.westlaw.com/Document/Ia69ed770208c11ebbea4f0dc9fb69570/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

[102] Ashley Murray, *City Council Approves Bill to Regulate Facial Recognition Technology*, Pittsburgh Post-Gazette (Sept. 23, 2020), *available at* https://1.next.westlaw.com/Document/I6048e330fd7211eaadd8fa89d4036ae0/View/FullText.html?transitionType=Default&contextData=(sc.Default).

[103] Prohibit the use of Face Recognition Technologies by private entities in places of public accommodation in the City, Ordinance No. 190114 (Sept. 9, 2020), *available at* https://efiles.portlandoregon.gov/Record/13945283.

[104] *See, e.g.*, Eric Newcomer, *California Will Be Key Battleground in Tech Privacy Fight in 2020*, Bloomberg (Jan. 2, 2020), *available at* https://www.bloomberg.com/news/articles/2020-01-02/privacy-fight-continues-in-california-dc-and-beyond.

[105] *Id.*

[106] *Id.*

[107] S. 4626, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/4626/text.

[108] Muge Fazlioglu, *Consolidating US Privacy Legislation: The SAFE DATA Act*, iAPP (Sept. 21, 2020), *available at* https://iapp.org/news/a/consolidating-u-s-privacy-legislation-the-safe-data-act/.

[109] 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.

[110] S. 2763, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/2763/text.

[111] S. 1084, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1084/text.

[112] S. 4626, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/4626/text.

[113] *Id.*

[114] S. 3456, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3456/text.

[115] *Id.*

[116] *Id.*

[117] H.R. 6675, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/6675/text.

[118] S. 2577, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/2577/text.

[119] H.R. 6675, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/6675/text.

[120] *Id.*

[121] *Id.*

[122] S. 3300, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3300/text.

[123] Eric Newcomer, *California Will Be Key Battleground in Tech Privacy Fight in 2020*, Bloomberg (Jan. 2, 2020), *available at* https://www.bloomberg.com/news/articles/2020-01-02/privacy-fight-continues-in-california-dc-and-beyond.

[124] S. 3300, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3300/text.

[125] *Id.*

[126] Data Accountability and Transparency Act of 2020 Staff Discussion Draft (2020), *available at* https://www.law360.com/articles/1284404/attachments/0.

[127] *Id.*

[128] *Id.*

[129] H.R. 6677, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/6677/text.

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, *available at* https://www.congress.gov/bill/116th-congress/house-bill/1668/text.

[139] Justin Katz, *Senate Passes IoT Cybersecurity Bill*, Federal Computer Week (Nov. 18, 2020), *available at* https://fcw.com/articles/2020/11/18/iot-cyber-bill-passes-senate.aspx.

[140] *Id.*

[141] *Id.*

[142] Chris Mills Rodrigo, *Booker, Merkley Propose Federal Facial Recognition Moratorium*, The Hill (Feb. 12, 2020), *available at* https://thehill.com/policy/technology/482815-booker-merkley-propose-facial-recognition-moratorium.

[143] S. 3284, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3284/text.

[144] *See* H.R. 7356, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/7356/text; S. 4084, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/4084/text.

[145] Press Release, Ed Markey United States Senator for Massachusetts, *Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology* (June 25, 2020), *available at* https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.

[146] *Id.*

[147] S. 4084, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/4084/cosponsors.

[148] H.R. 7356, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/7356/cosponsors.

[149] S. 4400, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/4400/actions.

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *See* H.R. 7891, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/7891/text; S. 4051, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/4051/text.

[154] 50 U.S.C. § 1861 (2018).

[155] 50 U.S.C. § 1801(b)(1)(C) (2015).

[156] 50 U.S.C. § 1805(c)(2)(B) (2018).

[157] H.R. 6172, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/6172/all-actions.

[158] Communications Decency Act of 1996, 47 U.S.C. § 230 (1996).

[159] *Id.*

[160] *See, e.g.*, Jessica Guynn, *Trump and Biden vs. Facebook: Why Section 230 could get repealed in 2021*, USA Today (Jan. 4, 2021), *available at* https://www.usatoday.com/story/tech/2021/01/04/trump-biden-pelosi-section-230-repeal-facebook-twitter-google/4132529001/ (describing political support for Section 230 reform or repeal in 2021).

[161] S. 3983, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3983/text.

[162] *Id.*

[163] Press Release, Marco Rubio U.S. Senator for Florida, *Rubio, Hawley Announce Bill Empowering Americans to Hold Big Tech Companies Accountable for Acting in Bad Faith* (June 17, 2020), *available at* https://www.rubio.senate.gov/public/index.cfm/press-releases?ContentRecord_id=47276D77-62D6-4E04-9FA2-1CD761179B90#:~

:text=The%20Limiting%20Section%20
230%20Immunity,if%20they%20violate%20those%20terms.

[164] S. 3398, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/3398/actions.

[165] *Id.*

[166] *Id.*

[167] *Id.*

[168] Press Release, Committee on the Judiciary, *Chairman Graham Applauds Senate Judiciary Committee for Unanimously Approving the EARN IT Act* (July 2, 2020), *available at* https://www.judiciary.senate.gov/press/rep/releases/chairman-graham-applauds-senate-judiciary-committee-for-unanimously-approving-the-earn-it-act#
:~:text=The%20EARN%20IT%20Act%20was,Against%20Online%20
Child%20Sexual%20Exploitation.%E2%80%9D.

[169] S. 4337, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/4337/text.

[170] *Id.*

[171] Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6505 (1998).

[172] Press Release, Federal Trade Commission, *FTC Seeks Comments on Children's Online Privacy Protection Act Rule: FTC to host workshop on COPPA in October as part of initiative* (July 25, 2019), *available at* https://www.ftc.gov/news-events/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule.

[173] H.R. 5573, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/5573/text.

[174] H.R. 5703, 116th Cong. (2020), *available at* https://www.congress.gov/bill/116th-congress/house-bill/5703/text.

[175] *Id.*

[176] 15 U.S.C. § 53(b); *see AMG Capital Mgmt., LLC v. Fed. Trade Comm'n*, No. 19-508, 2020 WL 3865250 (U.S. July 9, 2020).

[177] *See* Press Release, Federal Trade Commission, *FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information* (Dec. 14, 2020), *available at* https://www.ftc.gov/news-events/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services.

[178] *United States v. Facebook, Inc.*, 456 F. Supp. 3d 115 (D.D.C. 2020).

[179] *See* Press Release, Federal Trade Commission, *FTC Chairman's Statement Regarding the Court's Approval of the Facebook Settlement* (Apr. 24, 2020), *available at* https://www.ftc.gov/news-events/press-releases/2020/04/ftc-chairmans-statement-regarding-courts-approval-facebook.

[180] *See* Kate Conger, *F.T.C. Investigating Twitter for Potential Privacy Violations*, N.Y. Times (Aug. 3, 2020), *available at* https://www.nytimes.com/2020/08/03/technology/ftc-twitter-privacy-violations.html.

[181] Agreement Containing Consent, *In the Matter of Zoom Video Communications, Inc.*, File No. 1923167 (F.T.C. Nov. 9, 2020), *available at* https://www.ftc.gov/system/files/documents/cases/1923167zoomacco2.pdf.

[182] *See* Diane Bartz, *Exclusive: U.S. probing allegations TikTok violated children's privacy – sources*, Reuters (July 7, 2020), *available at* https://www.reuters.com/article/us-tiktok-privacy-children-exclusive/exclusive-u-s-probing-allegations-tiktok-violated-childrens-privacy-sources-idUSKBN248373.

[183] 15 U.S.C. § 53(b).

[184] *FTC v. Credit Bureau Ctr., LLC*, 937 F.3d 764 (7th Cir. 2019).

[185] *Id*. at 767.

[186] *Id*.

[187] *AMG Capital Mgmt., LLC v. Fed. Trade Comm'n*, No. 19-508, 2020 WL 3865250 (U.S. July 9, 2020).

[188] *AMG Capital Management, LLC v. FTC*, 910 F.3d 417 (9th Cir. 2018).

[189] Initially *Credit Bureau Center, LLC* and *AMG Capital Management, LLC* were consolidated to be heard together, but on November 9, the Supreme Court withdrew its consolidation order and vacated its order granting certiorari in *Credit Bureau Center, LLC*. *FTC v. Credit Bureau Ctr.*, No. 19-825, 2020 WL 6551765 (U.S. Nov. 9, 2020).

[190] *AMG Capital Management, LLC*, 910 F.3d at 426.

[191] Alexander Southwell, Ryan Bergsieker and Sarah Erickson, *Where Data Privacy And CFPB Are Headed Under Biden*, Law360 (Nov. 24, 2020), *available at* https://www.law360.com/articles/1331226/where-data-privacy-and-cfpb-are-headed-under-biden.

[192] Press Release, Department of Health and Human Services, *Health Insurer Pays $6.85 Million to Settle Data Breach Affecting Over 10.4 Million People* (Sept. 25, 2020), *available at* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/premera/index.html.

[193] Press Release, Department of Health and Human Services, *Health Care Provider Pays $100,000 Settlement to OCR for Failing to Implement HIPAA Security Rule Requirements* (Mar. 3, 2020), *available at* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/porter/index.html.

[194] Press Release, Department of Health and Human Services, *OCR Settles Five More Investigations in HIPAA Right of Access Initiative* (Sept. 15, 2020), *available at* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/right-of-access-initiative/index.html.

[195] Press Release, Department of Health and Human Services, *Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History* (Oct. 15, 2018), *available at* https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach.

[196] Steve Adler, *Court Approves Anthem $115 Million Data Breach Settlement*, HIPAA J. (Aug. 20, 2018), *available at* https://www.hipaajournal.com/court-approves-anthem-115-million-data-breach-settlement/.

[197] Press Release, Department of Health and Human Services, *OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* (Mar. 30, 2020), *available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

[198] Department of Health and Human Services, *FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency*, *available at* https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf.

[199] Press Release, Department of Health and Human Services, *OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency* (Apr. 9, 2020), *available at* https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-community-based-testing-sites.pdf.

[200] Press Release, Department of Health and Human Services, *OCR Issues Guidance on How Health Care Providers Can Contact Former COVID-19 Patients About Blood and Plasma Donation Opportunities* (Aug. 2020), *available* at https://www.hhs.gov/sites/default/files/guidance-on-hipaa-and-contacting-former-covid-19-patients-about-plasma-donation.pdf .

[201] New Release, Center for Medicare and Medicaid Services, *CMS Snapshot* (Aug. 27, 2020), *available at* https://www.cms.gov/files/document/snapshotupdate08272020.pdf.

[202] Press Release, Department of Health and Human Services, *HHS Proposes Modifications to the HIPAA Privacy Rule to Empower Patients, Improve Coordinated Care, and Reduce Regulatory*

Burdens (Dec. 10, 2020), *available at* https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/index.html.

[203] Department of Health and Human Services, *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement*, *available at* https://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf.

[204] Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 86 Fed. Reg. 6446 (published Jan. 21, 2021), *available at* https://www.federalregister.gov/documents/2021/01/21/2020-27157/proposed-modifications-to-the-hipaa-privacy-rule-to-support-and-remove-barriers-to-coordinated-care.

[205] Press Release, U.S. Securities and Exchange Commission, *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.

[206] *Id.*

[207] *Id.*

[208] SEC Office of Compliance Inspection and Examinations, *Cybersecurity and Resiliency Observations* (Jan. 27, 2020), *available at* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[209] Press Release, U.S. Securities and Exchange Commission, *SEC Announces Creation of the Event and Emerging Risk Examination Team in the Office of Compliance Inspections and Examinations and the Appointment of Adam D. Storch as Associate Director* (July 28, 2020), *available at* https://www.sec.gov/news/press-release/2020-165.

[210] U.S. Securities and Exchange Commission, *Cyber Enforcement Actions: Digital Assets/Initial Coin Offerings* (last updated Dec. 28, 2020), *available at* https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

[211] Final Judgment as to Defendants Telegram Group Inc. and Ton Issuer Inc., *SEC v. Telegram Group Inc. et al.*, 1:19-cv-09439 (S.D.N.Y. June 26, 2020), ECF No. 242.

[212] Opinion and Order, *SEC v. Telegram Group Inc. et al.*, 1:19-cv-09439 (S.D.N.Y. Mar. 24, 2020), ECF No. 227.

[213] *Id.*

[214] 328 U.S. 293 (1946).

[215] Opinion and Order, *SEC v. Kik Interactive Inc.*, 1:19-cv-5244 (S.D.N.Y. Sept. 30, 2020), ECF No. 88.

[216] *See, e.g.*, Complaint, *SEC v. Ackerman*, 1:20-cv-01181 (S.D.N.Y. Feb. 11, 2020), ECF No. 1 (complaint against Ohio-based businessman who allegedly orchestrated a digital asset scheme that defrauded approximately 150 investors, including many physicians); Complaint, *SEC v. Meta 1 Coin Trust, et al.*, 1:20-cv-00273 (W.D. Tex. Mar. 16, 2020), ECF No. 1 (complaint against an unincorporated entity purporting to be an irrevocable trust, a former state senator, and two others for allegedly conducting a fraudulent ICO of unregistered digital asset securities, and secured a temporary restraining order against the parties); Complaint, *SEC v. Dropil, Inc., et al.*, 8:20-cv-00793 (C.D. Cal. Apr. 23, 2020), ECF No. 1 (complaint against a digital currency company and its three founders for allegedly raising money from thousands of investors through a fraudulent ICO of unregistered digital asset securities); Complaint, *SEC v. FLiK, et al.*, 1:20-cv-03739 (N.D. Ga. Sept. 10, 2020), ECF No. 1 (complaint against several Georgia-based individuals who allegedly promoted two unregistered and fraudulent ICOs); *Tierion, Inc.*, Administrative Proceeding File No. 3-20188, Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Making Findings, and Imposing Penalties and a Cease-and-Desist Order (Dec. 23, 2020) (cease-and-desist proceeding against blockchain startup for unregistered offering of securities via "token sale"; company agreed to return funds to investors, pay $250,000 penalty, and disable trading in its "tokens").

[217] Complaint, *SEC v. Sotnikov, et al.*, 1:20-cv-02784 (D.N.J. Mar. 13, 2020), ECF No. 1; Press Release, U.S. Securities and Exchange Commission, *SEC Charges Russian National for Defrauding Older Investors of Over 26 Million in Phony Certificates of Deposit Scam* (Mar. 13, 2020), *available at* https://www.sec.gov/news/press-release/2020-61.

[218] *See id.*, Clerk's Entry of Default (Dec. 23, 2020) [electronic order], ECF No. 23

[219] Complaint, *SEC v. Ross*, 1:20-cv-05140 (N.D. Ga. Dec. 18, 2020), ECF No. 1; U.S. Securities and Exchange Commission, *SEC Charges Former Day Trader with Market Manipulation, Litigation Release No. 24989* (Dec. 18, 2020), *available at* https://www.sec.gov/litigation/litreleases/2020/lr24989.htm.

[220] Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, 47 U.S.C. § 227.

[221] 35 FCC Rcd 11186 (13) (2020).

[222] *Id.*

[223] *See Facebook, Inc. v. Duguid*, 141 S. Ct. 193 (2020).

[224] *See Carlton & Harris Chiropractic, Inc. v. PDR Network, LLC*, 982 F.3d 258 (4th Cir. 2020) (previously vacated and remanded by the Supreme Court in *PDR Network, LLC v. Carlton & Harris Chiropractic, Inc.*, 139 S. Ct. 2051 (2019)).

[225] Eric J. Troutman, *A Jarring Shift*, National Law Review (Dec. 11, 2020), *available at* https://www.natlawreview.com/article/jarring-shift-here-s-why-fourth-circuit-holding-fcc-tcpa-rulings-aren-t-entitled-to.

[226] *See, e.g.*, Notice of Apparent Liability in the Matter of Sprint Corp., 35 FCC Rcd 1655 (2) (2020); Notice of Apparent Liability in the Matter of T-Mobile USA, Inc., 35 FCC Rcd 1785 (2) (2020); Notice of Apparent Liability in the Matter of Verizon Comm., 35 FCC Rcd 1698 (2) (2020).

[227] Jennifer Valentino-DeVries, *Cellphone Carriers Face $200 Million Fine for Not Protecting Location Data*, N.Y. Times (Feb. 28, 2020), *available at* https://www.nytimes.com/2020/02/28/technology/fcc-cellphones-location-data-fines.html.

[228] Jennifer Valentino-DeVries, *Cellphone Carriers Face $200 Million Fine for Not Protecting Location Data*, NY Times (Feb. 28, 2020), *available at* https://www.nytimes.com/2020/02/28/technology/fcc-cellphones-location-data-fines.html.

[229] William Barr, *Statement of the Attorney General on the Announcement of Civil Antitrust Lawsuit Filed Against Google*, U.S. Dep't of Just. (Oct. 20, 2020), *available at* https://www.justice.gov/opa/pr/statement-attorney-general-announcement-civil-antitrust-lawsuit-filed-against-google.

[230] *Id.*

[231] Tony Romm, *US, States Sue Facebook as an Illegal Monopoly, Setting Stage for Potential Breakup*, Wash. Post (Dec. 9, 2020), *available at* https://www.washingtonpost.com/technology/2020/12/09/facebook-antitrust-lawsuit/.

[232] *See Cryptocurrency: Enforcement Framework*, Report of the Att'y Gen.'s Cyber Digital Task Force (Oct. 1, 2020), *available at* https://www.justice.gov/ag/page/file/1326061/download.

[233] *International Statement: End-To-End Encryption and Public Safety*, Dep't of Just. Office of Public Affairs (Oct. 11, 2020), *available at* https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

[234] *Id.*

[235] Russel Brandom, *US Joins Six Countries in New Call for Backdoor Encryption Access*, The Verge (Oct. 12, 2020), *available at* https://www.theverge.com/2020/10/12/21513212/backdoor-encryption-access-us-canada-australia-new-zealand-uk-india-japan.

[236] Jackson Barnett, *Final CMMC Acquisition Rule Goes Into Effect*, Fed Scoop (Dec. 1, 2020), *available at* https://www.fedscoop.com/cmmc-rule-change-goes-effect/.

[237] *Id.*

[238] Jackson Barnett, *The DoD Wants Better Cybersecurity for Its Contractors. The First Steps haven't Been Easy*, Fed Scoop (June 23, 2020), *available at* https://www.fedscoop.com/cmmc-dod-cybersecurity-requirments-contractors-timeline.

[239] *See, e.g.*, Jackson Barnett, *Final CMMC Acquisition Rule Goes Into Effect*, Fed Scoop (Dec. 1, 2020), *available at* https://www.fedscoop.com/cmmc-rule-change-goes-effect/.

[240] *See Ensuring American Leadership in Automated Vehicle Technologies*, A Report by the Nat'l Sci. & Tech. Council and the U.S. Dep't of Transportation (Jan. 2020), *available at* https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf.

[241] *Id.*

[242] Linda Chiem, *NHTSA Eyes New Self-Driving Car Regulatory Framework*, Law360 (Nov. 23, 2020), *available at* https://www.law360.com/articles/1331573/nhtsa-eyes-new-self-driving-car-regulatory-framework.

[243] *Id.*

[244] *See* Nat'l Inst. of Standards and Tech., *Foundational Cybersecurity Activities for IoT Device Manufacturers*, NISTIR 8259 (May 2020); Nat'l Inst. of Standards and Tech., *IoT device Cybersecurity Capability Core Baseline*, NISTIR 8259A (May 2020).

[245] Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207.

[246] Press Release, New York Attorney General, *Attorney General James Helps Secure $39.5 Million After Anthem's 2014 Data Breach* (Sept. 30, 2020), *available at* https://ag.ny.gov/press-release/2020/attorney-general-james-helps-secure-395-million-after-anthems-2014-data-breach.

[247] *Id.*

[248] *Id.*

[249] Press Release, New York Attorney General, *Attorney General James Helps Secure $17.5 Million After Data Breach at The Home Depot* (Nov. 24, 2020), *available at* https://ag.ny.gov/press-release/2020/attorney-general-james-helps-secure-175-million-after-data-breach-home-depot.

[250] *Id.*

[251] *Id.*

[252] Press Release, New York Attorney General, *Attorney General James Secures New Protections, Security Safeguards for All Zoom Users* (May 7, 2020), *available at* https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users.

[253] Danny Hakim & Natasha Singer, *New York Attorney General Looks Into Zoom's Privacy Practices*, N.Y. Times (Mar. 30, 2020), *available at* https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html.

[254] Press Release, New York Attorney General, *Attorney General James Secures New Protections, Security Safeguards for All Zoom Users* (May 7, 2020), *available at* https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users.

[255] Press Release, Arizona Attorney General, *Attorney General Mark Brnovich Files Lawsuit Against Google Over Deceptive and Unfair Location Tracking* (May 27, 2020), *available at* https://www.azag.gov/press-release/attorney-general-mark-brnovich-files-lawsuit-against-google-over-deceptive-and-unfair.

[256] *Id.*

[257] *Id.*

[258] Ruling, *State of Arizona, et al. v. Google LLC*, CV 2020-006219 (Super. Ct. Ariz. Maricopa Cnty. Sept. 25, 2020), *available at* https://www.azag.gov/sites/default/files/2020-10/CV2020-006219-926-09252020.pdf.

[259] Press Release, Office of Attorney General Maura Healey, *AG Healey Announces New Division Focused on Protecting Data Privacy and Security of Massachusetts Consumers* (Aug. 13, 2020), *available at* https://www.mass.gov/news/ag-healey-announces-new-division-focused-on-protecting-data-privacy-and-security-of.

[260] Twitter Investigation Report, N.Y. Dep't Fin. Serv., *Report on Investigation of Twitter's July 15, 2020 Cybersecurity Incident and the Implications for Election Security* (Oct. 14, 2020), *available at* https://www.dfs.ny.gov/Twitter_Report.

[261] In the Matter of First American Title Insurance Company, No. 2020-0030-C (July 21, 2020), *available at* https://www.law360.com/articles/1301950/attachments/0.

[262] *Id.*

[263] *Id.*

[264] *See, e.g.*, First American, "First American Reports Completion of Investigation into Customer Impact of Information Security Incident," July 16, 2019, *available at* https://web.archive.org/web/20190827180436/https://www.firstam.com/incidentupdate/update20190716.html.

[265] *Id.*

[266] Twitter Investigation Report, N.Y. Dep't Fin. Serv., *Report on Investigation of Twitter's July 15, 2020 Cybersecurity Incident and the Implications for Election Security* (Oct. 14, 2020), *available at* https://www.dfs.ny.gov/Twitter_Report.

[267] *Id.*

[268] *Id.*

[269] Press Release, N.Y. Dep't Fin. Serv., *Superintendent Lacewell Announces DFS to Host First-Ever Techsprint to Advance the Department's Regulator of the Future Vision* (Oct. 15, 2020), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202010151.

[270] *Id.*

[271] *Id.*

[272] *See* Risk-Based 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.

[273] Twitter Investigation Report, N.Y. Dep't Fin. Serv., *Report on Investigation of Twitter's July 15, 2020 Cybersecurity Incident and the Implications for Election Security* (Oct. 14, 2020), *available at* https://www.dfs.ny.gov/Twitter_Report.

[274] *See, e.g.*, Christopher Bing, *Suspected Russian Hackers Spied on U.S. Treasury Emails – Sources*, Reuters (Dec. 13, 2020), *available at* https://www.usnews.com/news/top-news/articles/2020-12-13/exclusive-us-treasury-breached-by-hackers-backed-by-foreign-government-sources.

[275] Mot. to Dismiss Pls.' First Am. Consolidated Shareholder Derivative Compl. Pursuant to Fed. R. Civ. P. 23.1 Or in the Alternative to Stay, *In Re Facebook, Inc. Shareholder Derivative Privacy Litigation*, No. 4:18-cv-01792-HSG (N.D. Cal. Feb. 18, 2020), ECF No. 145.

[276] Plaintiff's Opp. to Facebook's Mot. to Dismiss Plaintiff's First Amended Consolidated Shareholder Derivative Complaint, *In Re Facebook, Inc. Shareholder Derivative Privacy Litigation*, No. 4:18-cv-01792-HSG (N.D. Cal. Apr. 20, 2020), EFC No. 153; s*ee also* Emilie Ruscoe, Citing Zuckerberg's 'Iron Glove,' Facebook Investors Urge Trial, Law360 (Apr. 21, 2020), *available at* https://www.law360.com/articles/1265937.

[277] Order Adopting Report and Recommendation, *B.F. and A.A. v. Amazon.com Inc.*, No. C19-910 RAJ-MLP (W.D. Wa. Apr. 9, 2020), ECF No. 137.

[278] *Id.*

[279] *Drieu v. Zoom Video Communications, Inc.*, Case No. 3:20-cv-02353 (N.D. Cal. Apr. 7, 2020), ECF. No. 1.

[280] *Id.*

[281] *Id.*

[282] *Gervat v. Yuan et al.*, Case No. 1:20-cv-00797-LPS (D. Del. June 11, 2020), ECF. No. 1.

[283] *Id.*

[284] *Eugenio v. Berberian et al.*, Case No. 2020-0305-PAF (Del. Ch. Apr. 28, 2020).

[285] *Id.*

[286] *Id.*

[287] Complaint, *Brekhus v. Google LLC*, 5:20-cv-05488 (N.D. Cal. Aug. 7, 2020), ECF. No. 1.

[288] *Id* at 17.

[289] Plaintiff's Response in Support of Administrative Motion to Consider Whether Cases Should be Related, *Brekhus v. Google LLC*, 5:20-cv-05488-NC (N.D. Cal. Aug. 18, 2020), ECF No. 10.

[290] Complaint, *Allen v. Blackbaud, Inc.*, Case No. 2:20-cv-2930-RMG (D.S.C. Aug. 12, 2020), ECF No. 1.

[291] *Id.*

[292] *Id.*

[293] *Id.*

[294] *Hollett v. Gilmore et al.*, Case No. 1:20-cv-01620-UNA (D.S.C. Nov. 25, 2020), ECF. No. 1.

[295] *Id.*

[296] *Id.*

[297] *Id.*

[298] Order Granting Final Approval of Settlement, *In re Google Street View Elec. Commc'ns Litig.*, Case No. 10-md-02184-CRB (N.D. Cal. Mar. 18, 2020), ECF No. 184.

[299] *Id.*

[300] *Benjamin Joffe, et al v. Google, Inc.*, Case No. 20-15616 (9th Cir. 2020).

[301] *In re Google Plus Profile Litig.*, Case No. 5:18-cv-06164-EJD (N.D. Cal. June 10, 2020), ECF No. 13.

[302] *Id.*

[303] *In re Yahoo! Inc. Customer Data Security Breach Litig.*, Case No. 5:16-md-02752-LHK (N.D. Cal. July 22, 2020), ECF No. 497.

[304] *Id.* (comparing settlement to the settlement in *In re Anthem, Inc. Data Breach Litigation*, 327 F.R.D. 299 (N.D. Cal. 2018)).

[305] *Id.*

[306] 18 U.S.C. § 1030(a)(2).

[307] *See EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577, 581–83 (1st Cir. 2001); *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258, 1263–64 (11th Cir. 2010).

[308] *See United States v. Valle*, 807 F.3d 508, 523-28 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012); *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F.3d 756, 759–62 (6th Cir. 2020); *United States v. Nosal*, 676 F.3d 854, 856–64 (9th Cir. 2012) (en banc).

[309] Order List at 3, *United States v. Van Buren*, No. 19-783 (U.S. Apr. 20, 2020).

[310] Petition for Writ of Certiorari, *Van Buren*, No. 19-783 (U.S. Dec. 18, 2019).

[311] *Id.*; Order, *Van Buren*, No. 19-783 (U.S. Apr. 20, 2020).

[312] Transcript of Oral Argument at 48, 54, *Van Buren*, No. 19-783 (U.S. Nov. 30, 2020).

[313] Petition for Writ of Certiorari at 2–5, *LinkedIn Corp. v. hiQ Labs, Inc.*, No. 19-1116 (U.S. Mar. 9, 2020).

[314] *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003–04 (9th Cir. 2019).

[315] Petition for Writ of Certiorari at 3, *LinkedIn Corp. v. hiQ Labs, Inc.*, No. 19-1116 (U.S. Mar. 9, 2020).

[316] 451 F. Supp. 3d 73 (D.D.C. 2020).

[317] *Id.* at 88.

[318] Notice of Appeal, *Sandvig v. Barr*, No. 1:16-cv-01368 (D.D.C. May 26, 2020).

[319] *Glasser v. Hilton Grand Vacations Co.*, 948 F.3d 1301, 1306 (11th Cir. 2020); *see also ACA Int'l v. Federal Commc'ns Comm'n*, 855 F.3d 687 (D.C. Cir. 2018); *Dominguez v. Yahoo, Inc.*, 894 F.3d 116 (3d Cir. 2018).

[320] *Glasser*, 948 F.3d at 1306.

[321] *Id.*

[322] *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458 (7th Cir. 2020); *see also Glasser v. Hilton Grand Vacations Co.*, 948 F.3d 1301, 1306 (11th Cir. 2020); *ACA Int'l v. Federal Commc'ns Comm'n*, 855 F.3d 687 (D.C. Cir. 2018); *Dominguez v. Yahoo, Inc.*, 894 F.3d 116 (3d Cir. 2018).

[323] *Marks v. Crunch San Diego, LLC*, 904 F.3d 1041 (9th Cir. 2018).

[324] *Duran v. La Boom Disco, Inc.*, 955 F.3d 279 (2d Cir. 2020).

[325] *Allan v. Pennsylvania Higher Education Assistance Agency*, 968 F.3d 567 (6th Cir. 2020).

[326] *Facebook, Inc. v. Duguid*, 141 S. Ct. 193 L. Ed. 2d 1118 (2020) (granting certiorari).

[327] Christopher Cole, *Gov't Backs Facebook's View of Autodialers at High Court*, Law360 (Sept. 4, 2020), *available at* https://www.law360.com/articles/1307716/gov-t-backs-facebook-s-view-of-autodialers-at-high-court.

[328] *Facebook, Inc. v. Duguid*, No. 19-511 (U.S. Dec. 8, 2020) (arguments heard).

[329] *Barr v. American Ass'n of Pol. Consultants, Inc.*, 140 S. Ct. 2335 (2020).

[330] *Id.* at 2341, 2353–56.

[331] *Id.* at 2346.

[332] *Id.*

[333] *Id.* at 2356–57.

[334] *Id.* at 2343, 2353–56.

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

[336] Complaint for Damages and Equitable Relief, *In re: Zoom Video Commc'ns, Inc. Priv. Litig.*, No. 5:20-cv-02155 (N.D. Cal. Mar. 30, 2020), ECF No. 1. Note, the case was originally filed as *Cullen v. Zoom Video Communications, Inc.* before it was consolidated.

[337] *Id.*

[338] *Id.*

[339] First Amended Consolidated Class Action Complaint, *In re Zoom Video Commc'ns, Inc. Priv. Litig.*, No. 5:20-cv-02155 (N.D. Cal. Oct. 28, 2020), ECF No. 126.

[340] Defendant Zoom Video Communications, Inc.'s Notice of Motion and Motion to Dismiss the First Amended Consolidated Class Action Complaint; Memorandum of Points and Authorities in Support Thereof, *In re Zoom Video Commc'ns, Inc. Priv. Litig.*, No. 5:20-cv-02155 (N.D. Cal. Dec. 2, 2020), ECF No. 134.

[341] Class Action Complaint, *Hayden v. The Retail Equation, Inc.*, 8:20-cv-01203 (C.D. Cal. July 7, 2020), ECF No. 1.

[342] *Id.* In the plaintiffs' amended complaint, they now allege that several additional retailers shared data with The Retail Equation. First Amended Class Action Complaint, *Hayden v. The Retail Equation, Inc.*, 8:20-cv-01203 (C.D. Cal. Aug. 3, 2020), ECF No. 15.

[343] *Id.*

[344] *Id.*

[345] *See, e.g.*, Defendant The Gap, Inc.'s Notice of Motion and Motion to Compel Individual Arbitration and to Dismiss; Memorandum of Points and Authorities, *Hayden v. The Retail Equation, Inc.*, 8:20-cv-01203 (C.D. Cal. Nov. 6, 2020), ECF No. 140.

[346] *Id.* In the plaintiffs' amended complaint, they now allege that several additional retailers shared data with The Retail Equation. First Amended Class Action Complaint, *Hayden v. The Retail Equation, Inc.*, 8:20-cv-01203 (C.D. Cal. Aug. 3, 2020), ECF No. 15.

[347] Cal. Civ. Code §§1798.81.5(d)(1), 1798.140(o)(1), 1798.150(a)(1).

[348] Class Action Complaint, *Gupta v. Aeries Software, Inc.*, No. 8:20-cv-00995 (C.D. Cal. May 28, 2020), ECF No. 1.

[349] *Id.*

[350] Defendant Aeries Software, Inc.'s Notice of Motion and Motion to Dismiss Complaint Pursuant to Federal Rule of Civil Procedure 12(b)(6); Memorandum of Points and Authorities in Support, *Gupta v. Aeries Software, Inc.*, No. 8:20-cv-00995 (C.D. Cal. July 21, 2020), ECF No. 20.

[351] *Id.*

[352] Order Granting Joint Stipulation to Stay Litigation Through January 4, 2021, *Gupta v. Aeries Software, Inc.*, No. 8:20-cv-00995 (C.D. Cal. Nov. 24, 2020), ECF No. 40.

[353] Cal. Civ. Code § 1798.115(d).

[354] Cal. Civ. Code §§ 1798.110, 1798.115, 1798.120.

[355] Cal. Civ. Code § 1798.150(c).

[356] Complaint for Damages and Injunctive Relief for Violations of: (1) Negligence (2) Violation of Cal. Bus. & Prof. Code § 17200 (3) Breach of Implied Contract (4) Unjust Enrichment (5) Public Disclosure of Private Facts (6) Violation of California Consumer Privacy Act (7) Violation of Consumer Remedies Act, *Sweeney v. Life on Air, Inc.*, No. 3:20-cv-00742 (S.D. Cal. Apr. 17, 2020), ECF No. 1.

[357] *Id.*

[358] Order Granting Defendants' Motion to Compel Arbitration, *Sweeney v. Life on Air, Inc.*, No. 3:20-cv-00742 (S.D. Cal. Aug. 4, 2020), ECF No. 15.

[359] Class Action Complaint and Demand for Jury Trial, *G.R. v. TikTok, Inc.*, No. 2:20-cv-04537 (C.D. Cal. May 20, 2020), ECF No. 1.

[360] *Id.*

[361] *Id.*

[362] Conditional Transfer Order (CTO-1), *G.R. v. TikTok, Inc*., No. 1:20-cv-05212 (N.D. Ill. May 20, 2020), ECF No. 26.

[363] Cal. Bus. & Prof. Code § 17200.

[364] Cal. Civ. Code § 1798.150(c); S. Judiciary Comm., AB-375, 2017-2018 Sess. (Cal. 2018).

[365] Class Action Complaint, *Burke v. Clearview AI, Inc.*, No. 3:20-cv-00370 (S.D. Cal. Feb. 27, 2020), ECF No. 1.

[366] *Id.*

[367] *In re Clearview AI, Inc., Consumer Priv. Litig.*, MDL No. 2967, 2020 WL 7382590 (J.P.M.L. Dec. 15, 2020).

[368] Complaint for: (1) Violation of the California Consumer Privacy Act § 1798.150 (2) Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. (3) Negligence (4) Breach of Contract (5) Breach of Implied Contract, *Atkinson v. Minted, Inc.*, No. 3:20-cv-03869 (N.D. Cal. June 11, 2020), ECF No. 1.

[369] *Id.*

[370] *Id.*

[371] Amended Stipulated Request for Order Changing Time Pursuant to Civil L.R. 6-2 and Order, *Atkinson v. Minted, Inc.*, No. 3:20-cv-03869 (N.D. Cal. Dec. 1, 2020), ECF No. 35.

[372] 740 Ill. Comp. Stat. Ann. 14/20 (West 2008).

[373] 129 N.E.3d 1197, 1206 (Ill. 2019).

[374] 958 F.3d 617, 626–27 (7th Cir. 2020).

[375] 2020 WL 6738112, at *1 (7th Cir. Nov. 17, 2020).

[376] *In re Facebook Biometric Info. Privacy Litig.*, 2020 WL 4818608, at *3 (N.D. Cal. Aug. 19, 2020).

[377] 740 Ill. Comp. Stat. Ann. 14/20 (West 2008).

[378] The Ninth Circuit has held that pleading a violation of either sections 15(a) or (b) is sufficient to constitute injury-in-fact. *Patel v. Facebook*, 932 F.3d 1264, 1273–74 (9th Cir. 2019). However, the Second Circuit held that alleging a BIPA violation does not meet the injury-in-fact requirement without a showing that biometric data has been compromised in some manner. *Santana v. Take-Two Interactive Software*, 717 Fed. App'x 12, 16–17 (2d Cir. 2017).

[379] *See, e.g.*, *Meegan v. NFI Indus., Inc.*, 2020 WL 3000281 (N.D. Ill. June 4, 2020); *Frisby v. Sky Chefs, Inc.*, 2020 WL 4437805 (N.D. Ill. Aug. 3, 2020); *Williams v. Jackson Park SLF*, LLC, 2020 WL 5702294 (N.D. Ill. Sept. 24, 2020); Complaint, *Bartucci v. 401 N. Wabash Venture*, No. 2020CH05502 (Ill. Cir. Ct. Aug. 24, 2020); Complaint, *Payne v. Yum! Brands, Inc.*, No. 2020CH06811 (Ill. Cir. Ct. Nov. 16, 2020).

[380] *Liu v. Four Seasons Hotel, Ltd.*, 138 N.E.3d 201, 207 (Ill. App. Ct. 2019).

[381] *See, e.g.*, *Acaley v. Vimeo, Inc.*, 464 F. Supp. 3d 959 (N.D. Ill. 2020).

[382] *See, e.g.*, *Miracle-Pond v. Shutterfly*, Inc., 2020 WL 2513099 (N.D. Ill. May 15, 2020); *Kuznik v. Hooters of America, LLC*, 2020 WL 5983879 (C.D. Ill. Oct. 8, 2020).

[383] *McDonald v. Symphony Bronzeville Park LLC*, 2020 WL 5592607 (Ill. App. Ct. Sept. 18, 2020).

[384] *Gail v. Univ. of Chi. Med. Ctr., Inc.*, 2020 WL 1445608, at *4–*5 (N.D. Ill. Mar. 25, 2020); *Peatry v. Bimbo Bakeries USA, Inc.*, 2020 WL 919202, at *3–*4 (Ill. Cir. Ct. Feb. 26, 2020).

[385] *Miller v. Southwest Airlines Co.*, 926 F3d 898, 903–04 (7th Cir. 2019).

[386] *See, e.g.*, *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960 (N.D. Ill. 2020); *Bray v. Lathem Time Co.*, 2020 WL 1492742 (C.D. Ill. Mar. 27, 2020); *Figueroa v. Kronos Inc.*, 2020 WL 4273995 (N.D. Ill. July 24, 2020).

[387] *Avery v. State Farm*, 835 N.E.2d 801, 184–87 (Ill. 2005).

[388] Complaint, *Jerinic v. Amazon.com*, No. 2020CH6036 (Ill. Cir. Ct. Sept. 28, 2020).

[389] Complaint, *H.K. v. Google*, No. 5:20-cv-02257-NC (N.D. Cal. Apr. 2, 2020), ECF No. 1.

[390] *See, e.g.*, *Stauffer v. Innovative Heights Fairview Heights, LLC*, 2020 WL 4815960 (S.D. Ill. Aug. 19, 2020); *Robertson v. Hostmark Hosp. Grp.*, 2019 WL 8640568, at *4 (Ill. Cir. Ct. July 31, 2019); *Heard v. THC-NorthShore, Inc.*, No. 17CH16918, at *10 (Ill. Cir. Ct. Dec. 12, 2019).

[391] No. 1-20-0563 (Ill. App. Ct.).

[392] Mot. to Reopen Discovery Pursuant to FRCP 1, 26, and 37, *In Re Google Location History Litig.*, No. 5:18-cv-05062-EJD (N.D. Cal. Sept. 30, 2020), ECF No. 151.

[393] *Id.*

[394] *Id.*

[395] Memorandum Opinion and Order, *Dinerstein v. Google Inc.*, No. 19 C 4311 (N.D. Ill. Sept. 4, 2020), ECF No. 85.

[396] Laurann Wood, "*Google, U. of Chicago Want Out of Patient Disclosure Suit*," Law360 (Aug. 28, 2019), *available at* https://www.law360.com/articles/1193298?scroll=1&related=1.

[397] Memorandum Opinion and Order, *Dinerstein v. Google Inc.*, No. 19 C 4311 (N.D. Ill. Sept. 4, 2020), ECF No. 85.

[398] Memorandum and Order, *Flynn v. FCA US LLC*, No. 15-cv-855-SMY (S.D. Ill. Mar. 27, 2020), ECF No. 650.

[399] *Id.*

[400] Linda Chiem, "Drivers Defend Standing In 7th Circ. Jeep-Hacking Class," Law360 (June 19, 2020), *available at* https://www.law360.com/articles/1285000?scroll=1&related=1.

[401] *See, e.g.*, Order, *Zak v. Bose Corp.*, No. 17-cv-02928 (N.D. Ill. May 27, 2020), ECF No. 110.

[402] Jeannie O'Sullivan, "NJ Judge Trims Samsung Privacy Suit Over Smart TVs," Law360 (Aug. 21, 2019), *available at* https://www.law360.com/articles/1191213?scroll=1&related=1.

[403] Order, *White et al. v. Samsung Elecs. Am. Inc. et al.*, Case 2:17-cv-01775-MCA-JAD (D. N.J. Mar. 24, 2020), ECF No. 131.

[404] *Id.*

[405] *Id.*

[406] *Id.*

[407] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.

[408] Order on Google's Motion to Dismiss and Motion for Judicial Notice, *Balderas v. Google Inc.*, Case No. 20-CV-0143-NDF (D. N.M. Sept. 25, 2020), ECF No. 34

[409] *Id.*

[410] Wendy Davis, "New Mexico Wants Appeals Court To Revive Privacy Claims Against Google," MediaPost (Nov. 30, 2020).

[411] Order Re Motions to Dismiss, *McDonald v. Kiloo*, No. 17-cv-04344-JD (N.D. Cal. May 22, 2019), ECF No. 270; Motion for Preliminary Approval of Settlement, *McDonald v. Kiloo*, No. 3:17-cv-04344-JD (L) (N.D. Cal. Aug. 5, 2020), ECF No. 363.

[412] *Id.*

[413] *Id.*; *see also* Craig Clough, "Disney, Viacom Agree To Limit Data Collection In Kids Apps," Law360 (Aug. 6, 2020).

[414] Press Release, "Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data without Parental Consent," Federal Trade Commission (June 4, 2020), *available at* https://www.ftc.gov/news-events/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it.

[415] Stipulated Order for Permanent Injunction and Civil Penalty Judgement, *FTC v. Google LLC*, no. 1:19-cv-02642 (D.D.C. Sept. 4, 2019), ECF No. 2.

[416] Kate Cox, "YouTube unlawfully violates kids' privacy, new $3.2B lawsuit claims," *Arstechnica* (Sept. 14, 2020), *available at* https://arstechnica.com/tech-policy/2020/09/google-faces-3-2b-lawsuit-over-claims-it-violated-childrens-privacy/.

[417] Complaint, *Wesch v. Yodlee Inc*., no. 3:20-cv-05991 (N.D. Cal. Aug. 25, 2020), ECF No. 1.

[418] Defendant Yodlee, Inc.'s Motion to Dismiss Pursuant to Federal Rule of Civil Procedure 12(b)(6), *Wesch v. Yodlee Inc.*, no. 3:20-cv-05991 (N.D. Cal. Nov. 4, 2020), ECF No. 31.

[419] *Id.*

[420] Complaint for Damages and Declaratory and Injunctive Relief, *Cottle v. Plaid Inc.*, no. 3:20-cv-03056 (N.D. Cal. May 4, 2020), ECF No. 1.

[421] *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

[422] *United States v. Gratkowski*, 964 F.3d 307, 310 (5th Cir. 2020).

[423] *Id.* at 311–13.

[424] *Id*. at 311–12.

[425] *Id.* at 312.

[426] 2020 WL 3270877, at *1 (D. Mass. June 17, 2020).

[427] *Id.* at *5.

[428] *Id.* at *2–5.

[429] 981. F.3d 961, 964 (11th Cir. 2020).

[430] *Id.* at 969.

[431] *United States v. Moalin*, 973 F.3d 977, 996 (9th Cir. 2020).

[432] *Id.* at 988–89.

[433] *Id.* at 989.

[434] 442 U.S. 735, 741 (1979).

[435] *Moalin*, 973 F.3d at 989–91.

[436] 138 S. Ct. 2206, 2221 (2018).

[437] *Moalin*, 973 F.3d at 991.

[438] *United States v. Hasbajrami*, 945 F.3d 641, 642 (2nd Cir. 2019).

[439] *Id.* at 646.

[440] *Id.* at 651.

[441] S. 3501, 116th Congress (2019–2020).

[442] 50 U.S.C. § 1861 (2018).

[443] 50 U.S.C. § 1801(b)(1)(C) (2015).

[444] 50 U.S.C. § 1805(c)(2)(B) (2018).

[445] 50 U.S.C. § 1861 (2018).

[446] 50 U.S.C. § 1801(b)(1)(C) (2015).

[447] 50 U.S.C. § 1805(c)(2)(B) (2018).

[448] *Id.*

[449] 18 U.S.C. § 2713.

[450] *Crime (Overseas Production Orders) Act 2019*, c. 5 (Eng.), *available at* https://www.legislation.gov.uk/ukpga/2019/5/pdfs/ukpga_20190005_en.pdf.

[451] 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-combatcriminals-and-terrorists.

[452] The U.S. Department of Justice, *Letter from Assistant Attorney General Stephen E. Boyd to Congress* (Jan. 16, 2020), *available at* https://www.justice.gov/dag/page/file/1236281/download.

[453] 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-negotiationcloud-act-agreement-us.

[454] 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.

[455] *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* (Austl.), *available at* https://www.legislation.gov.au/Details/C2020B00030; *see also* Explanatory Memorandum, Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Austl.), *available at* https://www.legislation.gov.au/Details/C2020B00030/Explanatory%20Memorandum/Text.

[456] *Inquiry Announcement*, The Australian Parliamentary Joint Committee on Intelligence and Security, *Telecommunications Legislation Amendment (International Production Orders) Bill 2020, available at* https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IPOBill2020.

[457] Deham Sadler, *Global data-sharing deal 'deeply flawed'*, InnovationAus (Apr. 6, 2020), *available at* https://www.innovationaus.com/global-data-sharing-deal-deeply-flawed.

[458] Press Release, Court of Justice of the European Union, *The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield* (July 16, 2020), *available at* https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[459] *Id.*

[460] Case C-311/18, *Schrems v. Data Protection Commissioner* (July 16, 2020), *available at* https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2015.398.01.0005.01.ENG.

[461] Press Release, Department of Commerce, *Joint Press Statement from U.S. Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders* (Aug. 10, 2020), *available at* https://www.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european.

[462] Press Release, noyb, *101 Complaints on EU-US transfers filed* (Aug. 17, 2020), *available at* https://noyb.eu/en/101-complaints-eu-us-transfers-filed.

[463] *See, e.g.*, Samantha Raudins, *Facial Recognition, Thermal Imaging Part of the New Normal*, Columbus Dispatch (July 31, 2020), *available at* https://www.dispatch.com/story/business/information-technology/2020/07/30/facial-recognition-thermal-imaging-part-of-future-with-coronavirus/112807346/.

[464] Inioluwa Deborah Raji & Joy Buolamwini, University of Toronto and Massachusetts Institute of Technology, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products* (2019), *available at* https://dam-prod.media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf.

[465] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2019), *available at* https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[466] Complaint, *State of Vermont v. Clearview AI, INC.*, No. 226-3-20 (Vt. Super. Ct. Mar. 10, 2020), *available at* https://ago.vermont.gov/wp-content/uploads/2020/03/Complaint-State-v-Clearview.pdf; Order Granting in Part and Denying in Part Clearview AI's Motion to Dismiss, *State of Vermont v. Clearview AI, INC.*, No. 226-3-20 (Vt. Super. Ct. Sept. 10, 2020), *available at* https://ago.vermont.gov/wp-content/uploads/2020/09/Clearview-Motion-to-Dismiss-Decision.pdf.

[467] Complaint, *Am. Civil Liberties Union et al. v. Clearview AI, INC.*, No. 9337839 (Cir. Ct. Ill. Sept. 25, 2020).

[468] Press Release, New York Police Department, *NYPD Announces Facial Recognition Policy* (Mar. 13, 2020), *available at* https://www1.nyc.gov/site/nypd/news/pr0313/press-release---nypd-facial-recognition-policy.

[469] *Id.*

[470] Richard Winton et al., *LAPD Bars Use of Third-Party Facial Recognition Systems, Launches Review after Buzzfeed Inquiry*, L.A. Times (Nov. 17, 2020), *available at*

https://www.latimes.com/california/story/2020-11-17/lapd-bars-outside-facial-recognition-use-as-buzzfeed-inquiry-spurs-investigation.

[471] *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 979 F.3d 219, 224 (4th Cir. 2020).

[472] *Id*.

[473] *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 456 F. Supp. 3d 699, 703 (D. Md.); *See Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

[474] *Leaders of a Beautiful Struggle*, 979 F.3d at 223.

[475] *Id*.

[476] *Id*. at 227.

[477] *Id*. at 232.

[478] *MDS & One Year Permitting Overview*, L.A. Dep't Transp. (Feb. 7, 2019), *available at* https://ladot.lacity.org/sites/default/files/2020-03/mds-developer-webinar-one-year-permitting-overview_03-06-19_revision.pdf.

[479] *See* Complaint, *Social Bicycles v. City of Los Angeles Dep't of Transp.*, No. 2:20-CV-02746 (C.D. Cal. Mar. 24, 2020), ECF No. 1.

[480] The deal made Uber a primary investor in Lime and gave Uber the option to purchase Lime in 2022. *See* Kea Wilson, "Lime Just Became the Biggest Micromobility Company in the World," StreetsBlog (May 11, 2020), *available at* https://usa.streetsblog.org/2020/05/11/lime-just-became-the-biggest-micromobility-company-in-the-world/.

[481] *See* Complaint, *Sanchez v. L.A. Dep't of Transp.*, No. 2:20-CV-05044 (C.D. Cal. June 8, 2020), ECF No. 1.

The following Gibson Dunn lawyers assisted in the preparation of this article: Alexander H. Southwell, Ryan T. Bergsieker, Howard S. Hogan, Roscoe Jones Jr., Timothy W. Loose, Ashley Rogers, Eric D. Vandevelde, Abbey A. Barrera, Cassandra Gaedt-Sheckter, Daniel E. Rauch, Samantha Abrams-Widdicombe, Amanda M. Aycock, Fernando Berdion-Del Valle, Allison Chapin, Iman Charania, Josiah Clarke, Sarah Erickson, Zoey Goldnick, Eric Hornbeck, Andrew Howard, Jordan Jacobsen, Jennifer Katz, Brendan Krimsky, Nicole Lee, Warren Loegering, Prachi Mistry, Lauren Navarro, Macey Olave, Sarah Pongrace, Reid Rector, Jacob Rierson, Sarah Scharf, Raquel Alexa Sghiatti, Collin James Vierra, Hayato Watanabe, Victoria Weatherford, Hannah Yim, and Lisa V. Zivkovic.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. 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:

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)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+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)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@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)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@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)
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)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.