GIBSON DUNN

U.S. Cybersecurity and Data Privacy Review and Outlook – 2025

Client Alert | March 14, 2025

This Review addresses (1) the regulation of privacy and data security, other legislative developments, enforcement actions by federal and state authorities, and new regulatory guidance; (2) trends in civil litigation around data privacy and security in areas including data breach, wiretapping, biometrics, anti-hacking and computer intrusion statutes, and TCPA; and (3) trends related to data innovations and governmental data collection. Information on developments outside the United States—which are relevant to domestic and international companies alike—will be covered in Gibson Dunn's forthcoming International Cybersecurity and Data Privacy Review and Outlook, and additional developments relevant to AI will be covered in the Artificial Intelligence Review and Outlook.

Related People

Jane Horvath

Cassandra L. Gaedt-Sheckter

Ashley Rogers

Natalie J. Hausknecht

Abbey A. Barrera

Michael Brandon

Becca Smith

Jacob U. Arber

Trenton J. Van Oss

Megan Hulce

Andrew V. Kuntz

Viola Li

Bina Nayee

Sarah Scharf

Nick Carey

Courtney Wang

Hayato Watanabe

Caelin Moriarity Miltko

Lucy Musson

Shannon Summer

Advait V. Ramanan

Sam Gensburg

Danilo Risteski

Marcus Seete

Amy Xi Shao

Emma Wexler

 I. INTRODUCTION Congress's continued failure to pass a comprehensive privacy law left the states—as well as federal agencies—to keep leading the charge in defining and regulating cybersecurity and privacy in the United States. The states embraced this charge in 2024—seven states enacted new comprehensive privacy laws, and four states' comprehensive privacy laws took effect. With 11 new comprehensive privacy laws slated to take effect in 2025 and 2026, 20 states and approximately half of the U.S. population will be covered by a state comprehensive privacy law by 2026. While the newly enacted laws generally follow a similar framework and share common core requirements, important variations are starting to emerge, which threaten to further complicate the already heavy compliance burden for companies operating across state lines. At the same time, there was a growing emphasis on children's online privacy and biometric data in 2024, and a number of states amended their existing comprehensive privacy law to reflect this focus. State regulators similarly pursued an aggressive enforcement agenda in 2024, with a notable focus on children's data/social media, biometric data, and data brokers. There was also significant legislative, rulemaking, and enforcement activity at the federal level in 2024. Notably, the Protecting Americans' Data from Foreign Adversaries Act (PADFAA), which prohibits data brokers from transferring American's sensitive personal data to certain foreign countries, was enacted and went into effect in 2024. In addition, numerous federal agencies—including the FTC, SEC, CFPB, DOJ, and HHS—promulgated privacy and data protection regulations and guidance on a range of issues, including children's online privacy, biometric data, health data, location data, data brokers/national security, and cybersecurity incident disclosure, among other issues. Many federal agencies also brought enforcement actions against companies for alleged privacy, data security, and related violations. While we expect some of these trends to continue in 2025 and beyond, particularly at the state level, the Trump administration's early policy changes—defined by deregulation of the technology industry, removal of what some consider historical barriers to innovation, and a reversal of Biden-era policies related to content moderation, AI and digital assets, among other things—signal a significant shift at the federal level that will inevitably shape state policy and enforcement priorities. Litigation likewise remained active in 2024, with a continued uptick in claims by private litigants and government entities related to data breaches, federal and state wiretapping laws, and state biometrics laws. Litigation is expected to continue in these areas in 2025. This Review contextualizes these and other 2024 developments by addressing: (1) the regulation of privacy and data security, other legislative developments, enforcement actions by federal and state authorities, and new regulatory guidance; (2) trends in civil litigation around data privacy and security in areas including data breach, wiretapping, biometrics, anti-hacking and computer intrusion statutes, and TCPA; and (3) trends related to data innovations and governmental data collection. Information on developments outside the United States—which are relevant to domestic and international companies alike—will be covered in detail by Gibson Dunn's forthcoming International Cybersecurity and Data Privacy Outlook . **II. REGULATION OF PRIVACY AND DATA SECURITY** The state comprehensive data privacy law expansion trend continued in 2024, with seven states enacting new laws: Minnesota, Nebraska, New Hampshire, New Jersey, Maryland, Kentucky, and Rhode Island. Comprehensive data privacy laws took effect in four states in 2024: Florida, Texas, Oregon, and Montana. In 2025, another eight states—Delaware, Iowa, Minnesota, Nebraska, New Hampshire, New Jersey, Tennessee, and Maryland—will see their laws go into effect, and laws will take effect in three more states—Indiana, Kentucky, and Rhode Island—in early 2026. At that point, the total number of effective comprehensive state privacy laws will be 20, just seven years after California enacted the trail-blazing California Consumer Privacy Act. In addition, at the time of this report, the Connecticut, Iowa, and Tennessee legislatures are in various states of amending their current laws and another 16 states are actively considering data privacy legislation, with drafting and negotiations in various phases, and states have continued to enact narrower sector-specific laws covering minors, biometric information, and health information. We discuss these laws below and highlight different states' approaches to

consumer rights. Some state governments have also demonstrated a commitment to enforcing their data privacy laws, and announced several significant enforcement actions in 2024. With the continued absence of comprehensive federal privacy legislation, we suspect that states will continue to actively enforce their respective privacy laws. We discuss state-level enforcement below in our State Agencies section.

A. Regulation of Privacy and Data Security

1. State Legislation and Related Regulations

a. New Comprehensive State Privacy Laws Passed in 2024

Since California enacted the first comprehensive state privacy law in 2018, 19 other states have followed suit with their own comprehensive privacy legislation. The pace of legislation has accelerated in recent years—while only five states enacted privacy laws between 2018-2022, eight enacted laws in 2023, and seven more in 2024. Currently, 16 other states are also considering privacy legislation: Alabama, Arkansas, Georgia, Hawaii, Illinois, Massachusetts, Mississippi, New Mexico, New York, Ohio, Oklahoma, Pennsylvania, South Carolina, Vermont, Washington, and West Virginia. The seven state privacy laws enacted in 2024—Minnesota, Nebraska, New Hampshire, New Jersey, Maryland, Kentucky, and Rhode Island—generally share the same basic requirements, providing consumers with rights to access, correct and delete their personal data, and opt out of targeted advertising, profiling, and the sale of personal data. Although these core elements remain consistent, certain states have introduced unique provisions. We discuss the state laws passed in 2024 that will go into effect in 2025 in more detail below. For analysis of comprehensive privacy laws that took effect in 2024 (including Florida, Texas, Oregon, and Montana), please refer to last year's review.

b. Comprehensive State Privacy Laws Becoming Effective in 2025

A few months into 2025, comprehensive state privacy laws for five states—Delaware, Iowa, Nebraska, New Hampshire, and New Jersey—have already gone into effect with three more—Tennessee, Maryland and Minnesota—coming online later this year. While these laws are largely coextensive with existing comprehensive privacy laws, they also contain distinguishing features, which we summarize below. Nebraska's and New Hampshire's laws are substantially similar to existing state privacy laws, so we do not summarize those. Delaware The Delaware Personal Privacy Act for the most part aligns with other states' laws, but notably does not provide entity-level exemptions for institutions of higher education or most nonprofit organizations, unless the nonprofit provides services to victims or witnesses of child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking.[1] Delaware—along with Minnesota (discussed below) and Oregon—also requires that, as part of a consumer access request, data controllers disclose to the consumer the list of specific third parties, rather than just the categories of third parties, to which a business has disclosed that consumer's personal data. Iowa The Iowa Consumer Data Protection Act differs from other comprehensive state privacy laws by omitting several widely adopted consumer rights.[2] Iowa does not mandate data protection assessments for processing activities involving "heightened risk of harm to consumers," which sets it apart from every other state except for Utah, which also does not have this requirement.[3] Consumers also lack the right to opt out of processing for targeted advertising and profiling. They do, however, have the right to opt out of the sale of personal data. Iowa also diverges from most states in the manner it requires consent to

collect and process sensitive data.[4] The common practice is for controllers to obtain opt-in consent, but Iowa requires pre-use notice with an opportunity for consumers to opt out prior to having their data collected. This approach is distinctly controller-friendly, setting the default presumption that controllers can collect sensitive consumer data unless the consumer takes action to opt out. Maryland Maryland's Online Data Privacy Act, which will take effect in October 2025, has some of the strictest requirements in the country.[5] It is the only state to prohibit the sale of sensitive personal information entirely. With respect to minors, Maryland prohibits the sale of their personal information and the processing of their personal information for targeted advertising.[6] Maryland defines a minor as anyone under the age of 18, as compared to 16 and under in California's and Virginia's comprehensive data privacy laws (among others). And, unlike other states, Maryland extends this obligation to any business that "knew *or should have known*" the consumer's age. Other states, like Texas and Connecticut, require actual knowledge or willful disregard of the consumer's age.[7] Minnesota Most states give consumers the right to opt out of automated processing that furthers a significant decision (such as an employment decision), but, with its Consumer Data Privacy Act, Minnesota is the first state to offer consumers the right to *question* these decisions.[8] Minnesota's right to question includes the ability to: (1) know the reason behind the decision, (2) know what actions the consumer might have taken to secure a different decision in the future, (3) review the personal data used, and (4) correct inaccurate personal data and have the decision reevaluated. As businesses become more reliant on automated programs to assist in decisionmaking, this "right to question" will be a unique area of compliance that companies operating in Minnesota will have to be ready for. New Jersey With the New Jersey Data Privacy Law, which we also covered in last year's update, New Jersey joins California and Colorado in the small group of states that grants rulemaking authority to a state agency.[9] New Jersey's privacy law authorizes its director of the Division of Consumer Affairs to promulgate implementing regulations under Senate Bill 332, allowing the state agency to create rules to better carry out the law's intended purpose. The state agency has not yet proposed any regulations under this authorization. Tennessee The Tennessee Information Protection Act, while largely similar to other comprehensive state privacy laws, is unique in that it recognizes an affirmative defense to a violation.[10] If a data controller either maintains and complies with a written policy that aligns with the National Institute of Standards and Technology privacy framework or has documented policies designed to safeguard consumer privacy, it may avail itself of this defense.[11]

c. State Privacy Frameworks and Trends

The recent wave of state privacy legislation shows that most states are converging on core obligations, but meaningful divides on specific issues are also emerging. This section examines some of the most important distinctions between state privacy laws and their implications for compliance.

i. Enforcement and Rulemaking Authority

All state privacy laws, except California, grant enforcement authority solely to the state attorney general, prohibiting private citizens from filing lawsuits. To date, public actions have only been filed in California and Texas, although other state Attorneys General continue to serve non-public violation notices, requests for information, or civil investigative demands, and this is expected to increase as more state laws go into effect. Only three states—California, Colorado, and New Jersey—have empowered state agencies to issue regulations related to their respective privacy laws.[12] While California and Colorado have already issued regulations, New Jersey only recently empowered its

Division of Consumer Affairs within the Department of Law and Public Safety to do so. Unlike California and Colorado, New Jersey did not set a deadline for passing regulations, making it uncertain whether and when the state will exercise its rulemaking authority.

ii. Scope of Automated Decisionmaking Regulations

All states with privacy laws (except Utah and Iowa) allow consumers to opt out of certain forms of automated decisionmaking. States typically define automated decisionmaking as the processing of personal information to analyze or predict personal aspects such as health or behavior in furtherance of a significant decision.[13] Some states restrict this right to "solely" automated decisionmaking, while others provide the right to opt out of automated decisionmaking more broadly. The statutory scope of these opt out rights will become increasingly important as businesses roll out new automated processing tools.

Opt-out right for "solely" automated decisionmaking[14]	Opt-out dec
Connecticut Delaware Florida Indiana Maryland Montana Nebraska New Hampshire Rhode Island Tennessee Texas	California* Minnesota N

Definition of "Sale" Every state with privacy laws imposes obligations on businesses that "sell" personal information. Some states define the "sale" of data as an exchange for "monetary or other valuable consideration," while others define sale as an exchange for "monetary consideration" only. These differences can have major impacts, particularly for businesses that participate in marketing cooperatives or other similar organizations that provide services in exchange for data, rather than payment.

Monetary or other valuable consideration[18]	Mone
California Colorado Connecticut Delaware Florida Maryland Minnesota Montana Nebraska New Hampshire New Jersey Oregon Rhode Island Texas	Indiana Iowa

Children Since the Children's Online Privacy Protection Act (COPPA) was enacted in 1998, state privacy law has generally considered children's data to be sensitive data subject to the COPPA Rule's requirement that businesses must obtain parental consent before collecting personal information from children under 13 years old.[20] However, in recent years, many state laws have expanded their youth privacy protections to include heightened opt-in consent requirements for teenagers under the age of 16, requiring businesses to get affirmative consent for targeted advertising or the sale of data. New Jersey and Minnesota extend the opt-in requirement to those under 17, and Delaware extends it to age 18. Maryland goes further than any other state by prohibiting targeted advertising and the sale of data entirely if a business "knew or should have known" that the individual is under 18.

Opt-in consent for sale of data or targeted advertising (for children under 16 years old)[21]	Opt-in consent for sale of data, targeted advertising, *and profiling* (for children under 16 years old)[22]	No
California Connecticut Delaware (<18) Minnesota (<17) Montana New Hampshire	New Jersey (<17) Oregon	

iii. Consumer Rights

Although most states offer consumers the right to opt out of targeted advertising and the right to access and delete their data, many states provide additional consumer protections. Most states require businesses to honor universal opt-out mechanisms, such as the Global Privacy Control. Universal opt-out mechanisms allow consumers to opt out of personal data sales and targeted advertising automatically, rather than adjusting their preferences on a site-by-site basis. By the end of January 2026, 11 states will require controllers to recognize universal opt-out mechanisms. California, Colorado, Delaware, Montana, Nebraska, and Texas currently have an active requirement. New Jersey, Minnesota, and Maryland will require controllers to recognize universal opt-out mechanisms in the second half of 2025, followed by Connecticut and Oregon in January 2026. Most laws require businesses to disclose the "categories" of third parties that receive consumer information (for example, advertisers or payment processors). Delaware, Minnesota, and Oregon, however, require businesses to disclose a list of *specific* third parties in response to an access request. In Rhode Island, no request is necessary—a business is required to post the list of specific third parties in a conspicuous location on its website. Delaware and New Jersey are notable for being the only two states that require businesses to actually delete information after receiving a consumer request to delete.[25] Most states allow data to be kept if it is de-identified or removed from non-exempt use cases.[26]

	States with requirement	States without requiremen
Universal opt-out mechanism[27]	California Colorado Connecticut Delaware Maryland Minnesota Montana Nebraska New Hampshire New Jersey Oregon Texas	Florida Indiana Iowa Kentucky R Island Tennessee Utah Virgin
Response to right to access must include a list of "**specific third parties**" that have received the consumer's personal data[28]	Delaware Minnesota Oregon Rhode Island (must be posted publicly)	California Colorado Connecticut F Indiana Iowa Kentucky Maryland M Nebraska New Hampshire New J Tennessee Texas Utah Virgin
Actual deletion required on request (not just de-identification or removal from non-exempt use cases)[29]	Delaware New Jersey	California Colorado Connecticut F Indiana Iowa Kentucky Maryla Minnesota Montana Nebraska N Hampshire Oregon Rhode Isla Tennessee Texas Utah Virgin

2. Other State Privacy Laws

In addition to the comprehensive state privacy laws discussed above, states have continued to legislate in specific sectors, particularly in relation to minors' data, biometric information, and employee social media data.

a. Florida's Online Protection for Minors Act

On March 25, 2024, Florida Governor Ron DeSantis signed legislation to ban social media platforms from allowing children aged 13 and under to create social media accounts. The law requires social media platforms to delete existing accounts for children under the age of 14, and allows minors who are 14 and 15 to have social media accounts only upon parental consent.[30] The law is effective as of January 1, 2025.[31] The law also imposes a range of other restrictions. Websites that publish "material harmful to minors"—which generally refers to "obscene" materials, like pornography—must verify the age of the person attempting to access the material.[32] Social media platforms must also verify the age of users, using "commercially reasonable method[s]" and conduct such age verification through an independent third party.[33] These third parties may not retain or use personal identifying information for other purposes than age verification, and must anonymize and protect personal identifying information from unauthorized access.[34] The

law has been challenged by three internet-industry groups, which cite First Amendment concerns. According to these plaintiffs, the law is unconstitutional as it restricts minors' access to speech and forces businesses to collect sensitive data.[35] The law is currently paused from enforcement until a preliminary injunction motion for one of the ongoing cases is resolved.[36]

b. Protecting Georgia's Children on Social Media Act of 2024

On April 23, 2024, Georgia Governor Brian Kemp also signed legislation imposing new restrictions on minors' internet usage. Under the Protecting Georgia's Children on Social Media Act of 2024, social media companies are required to prevent minors, defined as those under 16 years old,[37] from using their services without the "express consent" of a parent or guardian.[38] Social media companies are also required to use commercially reasonable efforts to verify the age of account holders.[39] The law goes into effect on July 1 of this year.[40] In addition to the age verification requirements, social media companies must make available, upon a parent or guardian's request, a list and description of features offered on their platforms that parents and guardians can utilize to censor or moderate content.[41] Regarding minors' personal data, social media platforms are prohibited from displaying any advertising to a minor based on their personal information, except age and location, and may not collect personal information from a minor's posts, content, messages, text, or usage activities other than what is "adequate, relevant, and reasonably necessary for the purposes for which such information is collected."[42]

c. Maryland's Kids Code

On May 9, 2024, Maryland Governor Wes Moore signed legislation requiring data protection impact assessments for the processing of children's data and default privacy settings for children. The law is effective as of October 1, 2024. The law defines "child" as any consumer under the age of 18.[43] It requires companies that operate online products that are "reasonably likely to be accessed by children" to provide, upon request of the Division of Consumer Protection of the Office of the Attorney General, a data protection impact assessment that identifies the purpose of an online product, how it uses children's data, and whether it is designed in a manner consistent with the best interests of children.[44] "Best interests of children" refers to the reasonable foreseeability of material physical, financial, psychological, or emotional harm to children; a highly offensive intrusion on children's reasonable expectation of privacy, or discrimination against children based on race, color, religion, national origin, disability, gender identity, sex, or sexual orientation.[45] The law also requires that these companies put in place default privacy settings that offer children a "high level of privacy," restricting companies' ability to profile minors or process unnecessary data.[46] On February 3, 2025, an internet-industry trade association filed a complaint against the Maryland Attorney General, alleging that the Maryland Kids Code violated the First Amendment and 14th amendment. The plaintiff remarked that the law "presents websites with an impossible choice: either proactively censor broad categories of constitutionally protected speech or force users to submit sensitive personal information." The plaintiff also takes issue with the law's data protection impact assessment, alleging a First Amendment violation for "compel[ling] speech in the form of a data impact statement." It additionally argues that the "reasonably likely to be accessed by children" and "best interests of children" standards are vague.[47] A ruling is expected in the coming weeks.

d. New York's SAFE for Kids Act

On June 20, 2024, New York Governor Kathy Hochul signed the Stop Addictive Feeds Exploitation (SAFE) For Kids Act, the first set of restrictions in the nation on purportedly addictive social media feeds for minors. “Minor” under the law means individuals under the age of 18.[48] The law mandates that, unless parental consent is granted, minors may not receive “addictive feeds,” which are defined as websites, online services, or applications in which multiple pieces of media are recommended, selected, or prioritized for display to a user based on information associated with them or their device, unless specifically requested by the user (i.e., through a manual search).[49] The law also creates restrictions on platforms that offer “addictive feeds” as a significant part of their services, prohibiting these platforms from sending notifications to minors about the “addictive feed” between the hours of twelve to six a.m. Eastern Time, unless they receive parental consent.[50] This law will go into effect 180 days after New York Attorney General Letitia James finalizes regulations necessary for implementation.

e. Illinois’ Amended Biometric Information Privacy Act

On August 2, 2024, Illinois Governor J.B. Pritzker signed into law amendments to the Illinois Biometric Information Privacy Act (BIPA). These amendments were effective immediately.[51] Principal among these amendments was the provision that collecting the same biometric data from an individual using the same method is considered a single BIPA violation, and disclosing the same biometric data from the same person to the same recipient using the same method constitutes another single violation.[52] The amendments were enacted in response to the Illinois Supreme Court’s holding in *Cothron v. White Castle* that separate claims accrue under BIPA each time a private entity collects, and each time a private entity discloses, a person’s biometric data without that person’s consent.[53] *Cothron*’s holding would have allowed damages to accrue exponentially, and the recent amendments aim to mitigate that possibility. Since the amendments were signed into law, several courts have differed on whether the amendments should apply retroactively.

f. Colorado’s Privacy of Biometric Identifiers and Data Bill

On May 31, 2024, Colorado Governor Jared Polis approved a bill expanding consumers’ privacy rights and controllers’ and processors’ privacy obligations to biometric identifiers and biometric data.[54] Specifically, the bill requires controllers to make available to the public, with limited exceptions, a written policy specifying for biometric data and biometric identifiers: i) a data retention schedule, ii) a protocol for responding to data security incidents, including notifying consumers (processors must have a protocol for notifying controllers),[55] and iii) guidelines for required deletion.[56] Biometric identifiers or biometric data must be deleted at the earliest of i) when the initial purpose for collection has been satisfied, ii) 24 months after the consumer last interacted with the controller, or iii) the earliest feasible date, which must be no more than 45 days (or up to 45 additional days) after storage is no longer necessary as determined by an at least once-yearly audit.[57] Under the bill, employers must receive employees’ consent, which employers must not require as a condition of employment, to collect and process biometric data or biometric identifiers unless collection and processing is reasonably expected for a job or background check or is to: i) grant access to locations or systems, ii) record the employees’ full work day hours, iii) improve workplace or employee safety or security, or iv) improve public safety or security in a crisis.[58] The bill also includes consumer rights and protections that are generally common requirements in state privacy laws, such as notice, consent, and access rights. Specifically, the bill prohibits a controller from collecting

biometric identifiers or biometric data unless the controller first discloses the collection, the specific purpose for collection, the length of retention, and, if the biometric identifier is being shared, the specific purpose for sharing.[59] The controller also must not share the biometric identifier unless the consumer consents to such sharing or requests the sharing to complete a financial transaction, the sharing is to a processor and is necessary for the purpose of collection, or the sharing is otherwise required by law.[60] The bill grants consumers the right to access their biometric data collected by a controller, including the categories of biometric data collected or shared, its sources, the purposes for its collection or sharing, and the identities of third parties with which the controller discloses the biometric data.[61] A controller is prohibited from purchasing a biometric identifier unless the purchase is unrelated to the service provided to the consumer, the controller pays the consumer and the consumer provides consent, and the controller cannot refuse to provide, or charge a different rate for, a service because a consumer did not consent to the collection or processing of its biometric identifier, unless such collection is necessary to provide the service.[62] The bill, which amends the Colorado Privacy Act (CPA), takes effect July 1, 2025.[63]

g. New York's Amended Labor Law

On September 14, 2023, New York Governor Kathy Hochul signed legislation amending the New York State Labor Law to restrict employers from accessing their employees' and job applicants' "Personal Accounts."[64] This law is currently in effect.[65] Personal Account under the law covers several popular social media applications, defined as "an account or profile on an electronic medium where users may create, share, and view user-generated content . . . exclusively for personal purposes."[66] The law applies to all employers operating in the state of New York, excluding law enforcement agencies, fire departments, and departments of corrections and community supervision.[67] The law prohibits employers from requesting, requiring, or coercing their employees or job applicants to provide a password, username, or other information to access a Personal Account, to access their Personal Accounts in their employer's presence, or to reproduce information from their Personal Accounts.[68] Employers are prohibited from retaliating against any employee or job applicant that refuses to provide such information.[69] The law still enables employers to retrieve employee or job applicant information for the purpose of investigating or reporting alleged misconduct, provided the information is in the public domain or voluntarily shared.[70] The law also enables employers to require employees to disclose access information to a Personal Account on the employer's internal information systems,[71] or to an account used for business purposes.[72]

h. California's Protecting Our Kids from Social Media Addiction Act

On September 20, 2024, California enacted its Protecting Our Kids from Social Media Addiction Act. The law prohibits operators of "addictive" internet-based services or applications from providing "addictive feeds" to minors, unless the operator does not have actual knowledge that the user is a minor or obtains verifiable parental consent to provide such feeds to the minor user.[73] The law also prohibits these operators from sending notifications to minor users between certain hours.[74] Operators are also required to annually disclose the number of minor users of its service or application.[75] This law was blocked from enforcement earlier this year, with the trial court concluding that the law was likely an unconstitutional restriction on protected speech. As of January 28, 2025, the Ninth Circuit has granted a permanent injunction against the law's enforcement, pending the defendants' appeal.[76]

i. Colorado and California's Amendments to the "Sensitive Data" Definition

On April 17, 2024, Colorado Governor Jared Polis signed a bill to expand the definition of "sensitive data" under the CPA to include "biological data" and "neural data," which went into effect on August 7, 2024. Similarly, on September 28, 2024, California passed a bill to amend the definition of "sensitive personal information" in the California Consumer Privacy Act to include "neural data," which went into effect immediately. Both laws define "neural data" to include information generated by measuring the activity of a consumer's central or peripheral nervous system.[77] Colorado requires that "neural data" "be processed by or with the assistance of a device,"[78] whereas California provides that "neural data" "is not inferred from nonneural information."[79] Both laws would apply to novel neurotechnology devices and more commonplace items like electroencephalograms (EEGs).[80] Colorado has gone one step further by including "biological data" in its definition of "sensitive information," which it defines as "data generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or activities or of an individual's body or bodily functions, which data is used or intended to be used, singly or in combination with other personal data, for identification purposes."[81]

3. Federal Legislation

a. Comprehensive Federal Privacy Legislation

Calls for comprehensive federal privacy legislation remain loud and unanswered, despite bipartisan congressional efforts to introduce new legislation. The comprehensive American Privacy Rights Act (APRA) was introduced on April 7, 2024, by a bipartisan and bicameral group of lawmakers, and attempts to create a unified data privacy standard addressing the collection and processing of personal data as well as data breaches.[82] As proposed, APRA would grant consumers the right to access, correct, delete, and export collected data and to know who their data is transferred to and the purpose for transfer.[83] The Congressional Research Service notes that APRA would also preempt state privacy laws, subject to certain exceptions. Since its introduction APRA has seen little movement, due to strong opposition from a variety of stakeholders and prioritization of other legislation. State regulators, such as the California Privacy Protection Agency, oppose APRA as it would preempt state laws in the same area. Certain interest groups opposed the removal of provisions relating to civil rights protections and algorithmic accountability. A last-minute cancellation of the House Committee on Energy and Commerce's scheduled markup of the APRA on June 27, 2024 was the last official action taken on the bill. While momentum for APRA has slowed, former FTC Chair Jon Leibowitz stated "[t]here's 85% agreement between Democrats and Republicans about what should be in it, so I expect real movement on privacy legislation, even if what goes through lacks a private right of action, for example." However, given the many other competing objectives of the new Trump Administration in the early days of the Administration, it is unlikely that a bill will be passed in the coming months.

b. Other Introduced Legislation

Congress passed only one privacy-related law in 2024, which focused on national security

issues, although a number of consumer and individual privacy-related laws were introduced. In April 2024, President Biden signed H.R. 815 into law, which included the Protecting Americans' Data from Foreign Adversaries Act of 2024.[84] PADFAA represents an effort to regulate the transfer of personal data from the U.S. due to national security concerns. The law, which went into effect on June 23, 2024, prohibits data brokers from selling, transferring, or disclosing personally identifiable sensitive data of a U.S. individual to any foreign adversary country (China, Russia, Iran, and North Korea) or any entity controlled by a foreign adversary country.[85] PADFAA defines "personally identifiable sensitive data" broadly as "any sensitive data that identifies or is linked or reasonably linkable, alone or in combination with other data, to an individual or a device that identifies or is linked or reasonably linkable to an individual."[86] Other proposed privacy legislation covered a range of topics—including workplace privacy, health privacy, financial privacy, privacy for children online, facial recognition, and AI—several of which attracted significant bipartisan support, but lawmakers remained divided over the same two issues that sunk more comprehensive federal privacy legislation: (1) whether federal privacy laws should preempt state laws (a position attracting more Republican support); and (2) whether it should include a private right of action (which more Democrats favor). Of the proposed privacy-focused legislation in 2024, much of the focus was on digital privacy and safety, especially for children on social media. Congress held widely publicized hearings on the topic, questioning social media executives on their failure to protect children online. In July 2024, the U.S. Senate overwhelmingly passed a pair of measures seeking to put more responsibility on social media platforms to ensure child safety online: The Kids Online Safety Act, which establishes a duty of care for online platforms and requires them to activate the most protective settings for kids by default, and the Children and Teens' Online Privacy Protection Act (COPPA 2.0), which amends COPPA. COPPA 2.0 extends existing COPPA protections by banning online companies from collecting personal information from teenage users over the age of 12 and under 17, and broadening the entities and services covered. It also makes it unlawful to collect and use personal information from children and teens in targeted advertisements while affording users a right to erasure of their content and imposes new obligations for businesses that collect personal information from children and teens. The full House of Representatives has yet to debate either bill and it is unclear if action will be taken in 2025 to move either forward. Other privacy bills introduced in 2024 include: The Verifying Kids' Online Privacy Act (amending COPPA to define a child as an individual under the age of 16 rather than 13 and requiring operators to verify the age of individuals accessing their service), the Stop Spying Bosses Act (requiring disclosure of or prohibiting surveillance, monitoring, and collection of worker data),[87] the No Robot Bosses Act (prohibiting employers from relying exclusively on automated decisionmaking systems to make decisions regarding employment),[88] the Reproductive Data Privacy and Protection Act (ensuring government entities that seek to compel disclosures relating to reproductive or sexual health information cannot do so for investigatory purposes),[89] the American Donor Privacy and Foreign Funding Transparency Act (restricting the ability of federal government entities to collect or require submission of information on the identification of donors to tax-exempt organizations),[90] the Protecting Privacy in Purchases Act (prohibiting payment card networks from requiring firearms retailers to use a merchant category code that would distinguish it from a general merchandise or sporting goods retailer),[91] and others described in this Review. Congress also considered cybersecurity-related legislation: The Healthcare Cybersecurity Act of 2024 (requiring the Cybersecurity and Infrastructure Security Agency and the Department of Health and Human Services to work together and implement a variety of measures to improve cyber defenses in the healthcare sector),[92] the Farm and Food Cybersecurity Act of 2024 (requiring studies and simulation exercise for food-related cyber emergencies, threats, and disruptions),[93] and the Health Infrastructure Security and Accountability Act (creating mandatory minimum cybersecurity standards for health care providers, health plans, clearinghouses, and business associates along with requiring independent audits).[94]

B. Enforcement and Guidance

In 2024, federal regulators continued to actively pursue enforcement action and

rulemaking related to cybersecurity and data privacy. This section summarizes the noteworthy efforts by the Federal Trade Commission (FTC), Consumer Financial Protection Bureau (CFPB), Securities and Exchange Commission (SEC), Department of Health and Human Services (HHS), and other federal and state agencies. The priorities reflected in federal enforcement actions and rulemakings will likely shift in 2025, as the newly appointed agency leaders implement the Trump Administration's policy agenda.

1. Federal Trade Commission

The FTC continued its active regulation and enforcement of cybersecurity and data privacy in 2024. A number of the FTC's litigation matters, many of which represented its focus on sensitive consumer data such as geolocation and health information, reached settlement. The impact of the agency's rulemaking can also be seen in its recent settlement agreements. For example, aspects of its Standards for Safeguarding Customer Information Rule (Safeguards Rule) were often cited in settlements of data privacy enforcement matters through terms, such as limiting an entities' agents' access to consumer information only where necessary. The FTC also launched, via orders pursuant to Section 6(b) of the FTC Act, fact-finding studies into eight companies to investigate how the companies use consumers' personal data to engage in personalized pricing—the practice of charging different customers different prices for the same good. In his concurring statement, Former Commissioner, and current Chair, Andrew Ferguson emphasized the primary goal of these studies as fact-finding rather than pursuing enforcement action or rulemaking. He suggested that any necessary remedial action should be left to Congress and state lawmakers. Other areas that the FTC prioritized included algorithmic bias and AI, commercial surveillance, data security, and children's privacy. Further, the FTC expanded its regulatory and enforcement scope related to biometric information. This section discusses the FTC's notable actions in 2024; however, it bears noting that the agency's outlook this year will be impacted by President Trump's February 18, 2025 executive order requiring independent agencies to consult with the White House about its strategic plans, priorities, and draft regulations. While the executive order expressly lists the FTC, SEC, and FCC as impacted agencies, the CFPB probably will be impacted as well if it is operational under the Trump administration.

a. FTC Organization Updates

On March 25, 2024, Republican Melissa Holyoak was sworn in as a Commissioner for the FTC, filling the seat left open by former Commissioner Christine Wilson in March 2023. Subsequently, on April 2, 2024, Republican Andrew Ferguson was sworn in as a Commissioner, filling the seat left open by former Commissioner Noah Phillips in October 2022. In December 2024, President Donald Trump announced he planned to appoint Commissioner Ferguson to replace then-Chair Lina Khan. During the same month, reports circulated with a leaked document that professed to lay out Ferguson's priorities for the agency, if he were selected as the Chair. Specifically, it stated Ferguson's "Agenda for the FTC" would: "Reverse Lina Khan's Anti-Business Agenda," with "no more novel and legally dubious consumer protection cases," and by "stop[ping] abus[e of] FTC enforcement authorities as a substitute for comprehensive privacy legislation"; "Hold Big Tech Accountable and Stop Censorship,"[95] including through focused antitrust enforcement; "Protect Freedom of Speech and Fight Wokeness," including by "end[ing] the FTC's attacks on online anonymity"; and "Fight the Bureaucracy to Implement Trump's Agenda." On January 20, 2025, President Trump appointed Andrew Ferguson as the new FTC Chairman. In December 2024, President Trump also announced he planned to nominate Mark Meador as the new Republican FTC commissioner to replace the seat left open by prior Chair Lina Khan, whose term expired on January 31, 2025. Meador is currently a partner at law firm Kressin Meador Powers and previously worked for the FTC and the DOJ and as Deputy Chief Counsel for Antitrust & Competition to Republican

Senator Mike Lee. Meador has vocally supported efforts to regulate big technology companies and has called for increased antitrust enforcement. If Meador is confirmed, the FTC will be led by a Republican majority for the first time since Commissioner Bedoya was confirmed in 2022.

b. Algorithmic Bias and Artificial Intelligence

Algorithmic bias has been a growing concern regarding the use of AI technology for the FTC under former FTC chair, Lina Khan. In 2023, Khan, in a guest editorial for the New York Times, expressed concern over AI tools being fed information "riddled with errors and bias," thereby "automating discrimination" and unfairly inhibiting people's access to financial services, employment, and housing, among others. In December 2023, the FTC filed a complaint and proposed stipulated order against a convenience store chain. The FTC alleged the chain used AI-based facial recognition technology (FRT) to identify customers who may have been engaging in shoplifting and other problematic behavior. In March 2024, the court entered the stipulated order, which prohibits the company from using FRT for five years. In December of 2024, the FTC once again filed a complaint and proposed stipulated order, this time against an AI and Deep Learning-based video analytics and video cloud software company, alleging that the company made false, misleading, or unsubstantiated claims that its AI-powered facial recognition software was free of gender or racial bias, and that it had one of the highest accuracy rates on the market despite lacking the evidence to support such claims. The complaint also alleged that the company did not train its FRT software on "millions of faces" as it advertised, but only on approximately 100 unique individuals. The FTC's finalized order against the company prohibits the company from misrepresenting the accuracy and efficacy of its technology without competent and reliable testing of the technology to support its claims, among other restrictions and requirements. Newly appointed Chair Ferguson has expressed his disagreement with the FTC's prior approach to AI, indicating his belief that the "pro-regulation side of the AI debate" is "the wrong one." For example, Chair Ferguson has expressed some disagreement with the FTC's approach to defining bias. In his statement concurring in the FTC's action against the AI and Deep Learning-based video analytics and video cloud software company, IntelliVision, he expressed discomfort with relying on "statistical disparity in false-positive and false-negative rates" to define or determine the presence of bias and instead focused on IntelliVision's failure to substantiate its claims that its software had "zero gender or racial bias."

c. Commercial Surveillance and Data Security

In 2023, as discussed in our prior alerts, the FTC issued an Advance Notice of Proposed Rulemaking on commercial surveillance and data security. In July 2024, the FTC issued orders to "eight companies offering surveillance pricing products and services . . . seek[ing] information about the potential impact these practices have on privacy, competition, and consumer protection." In January 2025, the FTC then released its initial findings in a surveillance pricing market study, which provided insights into the level of detail at which consumer behavior and demographics are surveilled and analyzed and the effects this has on surveillance pricing. That same day, the FTC announced it would open up public comments on its commercial surveillance probe, which, unrelated to any proposed rulemaking, asked for public input until April 17, 2025 from businesses and workers about their experiences or views on the impact of surveillance pricing. On January 22, 2025, Chair Ferguson closed public comments. The unexplained shutdown of public comments has been criticized by fellow FTC Commissioner Alvaro Bedoya. While Chair Ferguson has voiced support for the FTC's attempts to inform consumers regarding the extent of commercial surveillance, he has criticized the FTC's approach to targeted

advertising and AI arguing both that such targeted advertising is beneficial to consumers, and that mass data collection is difficult to avoid but also critical for the operation of many free internet services. The FTC may take a different approach to commercial surveillance concerns going forward. Both Chair Ferguson and Commissioner Melissa Holyoak dissented from the former Democratic majority in the FTC for what the Republican Commissioners perceived as rushing to publish the initial findings of the surveillance pricing study. Chair Ferguson and Commissioner Holyoak opined that it was irresponsible for the FTC to put forward such a preliminary "beta" version of their findings, just to publicize an FTC statement on the matter prior to the start of President Trump's term.

d. Notable FTC Enforcement Actions

In 2024, the FTC continued to aggressively enforce data privacy and the uses of sensitive consumer information. There are a few trends that businesses can observe as part and parcel of the agency's agenda last year—in case resolutions, the FTC required the entities collecting and using location and health information for non-essential functions to delete that data, and invest in significant privacy and data security programs. Irrespective of an administration change, the FTC likely will continue to focus on the failure to protect or the misuse of sensitive data—actions that Commissioner Holyoak has supported in multiple concurring statements she published supporting related FTC actions and settlements. ***Corporate Landlord of Single-Family Homes***. The FTC and a corporate landlord reached a settlement to resolve the FTC's allegations of undisclosed "junk fees," improper retention of tenants' security deposits and refunds, and misrepresentation of home inspection and maintenance practices. The company agreed to pay a $45 million fee that the FTC says will be used to refund impacted consumers. The company is also permanently restrained from mispresenting monthly lease pricing and fees, property conditions, and the circumstances under which it will deduct funds from consumers' security deposits. Consistent with the agency's recent focus on consumer data retention, the settlement requires the corporate landlord to delete all financial data collected from consumers outside limited circumstances. ***Digital Marketing and Data Aggregator***. After facing allegations of impermissibly collecting and using consumers' location data for advertising purposes, a marketing company reached a settlement with the FTC. The administrative complaint alleged the company failed to fully disclose to consumers how their location data, which would reveal where they live and work, would be used for purposes other than necessary app functions. The agreed-upon order prohibits the company from sharing in any way consumers' precise location data, or offering any product or service designed to target consumers based on their location. The FTC also required the company to destroy all stored location data or ensure the data is deidentified. ***Substance Abuse Telehealth Firms***. The DOJ settled an action it brought on behalf of the FTC against two telehealth companies for alleged violation of the Opioid Addiction Recovery Fraud Prevention Act of 2018 (OARFPA) through unfair and deceptive trade practices relating to alcohol and substance abuse treatment. In addition to the monetary penalties, the court-approved joint stipulations banning the companies from disclosing consumer health information to third parties for advertising purposes. The companies must also implement a privacy and data security program to formalize the process by which they keep health information secure, as well as a data retention schedule to limit the time period that they retain consumer data. ***Online Therapy***. In May 2024, an online therapy firm began issuing refund notifications to impacted consumers, based on a 2023 settlement with the FTC arising out of allegations that the firm shared consumers' sensitive data with third parties. The FTC has indicated that it considers sensitive consumer data to include email addresses, IP addresses, and answers to personal health questions. The online therapy provider was charged with sharing such consumer information with online and app advertisers without setting appropriate limitations for the advertisers' use of the data, and without obtaining consumer consent. ***Software Provider***. The FTC settled allegations against a UK-based software provider that its Czech subsidiary collected and sold consumer browsing information without adequate notice and

consent. The subsidiary is alleged to have sold the browsing data to more than 100 third parties. As per the final order, the company and its subsidiaries are required to delete the copies of the data that was sold, and to obtain consent from future consumers before selling browsing data for advertising purposes. ***Data Brokers***. The FTC brought a second amended complaint against a data broker for allegedly violating Section 5 of the FTC Act by selling consumers' precise location data. The second amended complaint comes after the presiding federal district court judge denied the data broker's attempt to dismiss the suit. In her concurring statement in support of the Commission's vote to file the amended pleading, Commissioner Holyoak underscored the importance of "vigorously pursuing" the action in order to protect precise geolocation information identifying consumers' visits to sensitive locations. A separate data broker also agreed to settle FTC claims that it unlawfully tracked and sold sensitive location data. The Commission voted 5-0 to approve the final order, which prohibits the data broker from selling sensitive location data or collecting such data, outside a limited number of approved purposes. ***Security Camera Company***. The DOJ settled an action it brought on behalf of the FTC against a security camera company that is alleged to have violated the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM). The company is also alleged to have had insufficient security measures over consumer data it collected, allowing a hacker to access customers' security camera data in 2021. The hacker is alleged to have accessed cameras in particularly sensitive locations such as psychiatric hospitals and women's health clinics. The company agreed to pay a $2.95 million monetary penalty for its CAN-SPAM violation and implement an information privacy program, among other actions. ***Smart Home Technology***. In December, the FTC sent the first set of payments to consumers allegedly harmed by a home security company's misuse of credit reports. The company, which agreed to a settlement with the FTC in 2021, paid $5 million to be disbursed directly to consumers. According to the FTC, the company's sales representatives relied on false or unverified information to help consumers get financing approval for products and services that they would not otherwise be qualified to receive. The FTC's December payment of nearly $500,000 is directed to 470 consumers, who filed a valid claim. Additional funds are stated to be distributed at a later date.

e. Financial Privacy

Pursuant to Section 6(b) of the FTC Act, the FTC issued orders to eight firms, including financial services firms, that advertise using customer information and machine learning technologies to engage in targeted pricing to consumers. The orders require recipient companies to disclose documents showing how they use consumer data, such as credit history, to engage in "surveillance pricing," also known as "personalized pricing." This pricing practice involves charging different prices for the same product based on the consumer's personal data. The firms were mandated to provide documents and information relating to four specific aspects of their personalized pricing:

- The types of products and services offered using personalized pricing;
- The personalized pricing offerings' underlying data and how such data was collected;
- Targeted clients and their use of the offerings; and
- Resulting pricing differentials for the same offering and other impacts.

In a concurring statement, then-Commissioner Ferguson underscored the primary goal of these studies as gathering information rather than pursuing enforcement actions, expressing the importance of revealing to Congress and the public "whether and how consumers' private data may be used to affect their pocketbooks." He voiced less enthusiasm for the Commission taking remedial action based on the studies' outcome, suggesting instead that state and federal legislators may address any needed response

through privacy laws. In addition to launching the personalized pricing study, the FTC began to incorporate aspects of its Safeguards Rule in case resolutions. Settlement agreements of actions involving unsecured consumer information, in particular, reflect certain components of the Safeguards Rule. For example, a common settlement term requires companies to implement information privacy programs and abstain from misleading consumers about the strength and integrity of their consumer privacy measures. One important feature of these programs is that the entity must place limitations on an employee's, contractor's, and authorized third parties' access to consumer information based on job necessity.

f. Children's and Teens' Privacy

At the end of 2023, the FTC proposed amendments to COPPA, aiming to shift the burden for protecting children's privacy and security from parents to service providers. As of January 16, 2025, the FTC finalized changes to COPPA. The final rule's amendments include:

- Opt-in parental consent requirements for covered operators to disclose children's personal information to third-party companies for targeted advertising or other purposes;
- Limits on data retention where covered operators may only retain personal information for as long as reasonably necessary to fulfill a specific purpose for which it was collected;
- Public disclosure requirements for COPPA's self-regulatory Self-Harbor programs, such as disclosure of information on their membership lists; and
- Several amended definitions, including the expansion of "personal information" to include biometric identifiers and government-issued identifiers.

In adopting the final rule, the FTC decided against adopting some proposed changes it received during the public comment period, such as a requirement to limit the use of push notifications directed to children without parental consent and changes to requirements applicable to educational technology companies that operate in a school environment. In 2023, the FTC also sought comment on the Entertainment Software Rating Board's (ESRB) application for a "Privacy-Protective Facial Age Estimation" technology that analyzes a user's face to confirm their age, which would serve as a consent mechanism under COPPA's requirement that parents consent to an online service collecting their children's personal data. On March 29, 2024, the FTC denied the ESRB's application with a vote of 4-0 due to insufficient information. The FTC made this denial without prejudice to enable the ESRB to re-file the application in the future, when the FTC anticipates that additional information will assist in the understanding of age verification technologies. The FTC otherwise took no position on the merits of the application. In 2024, the FTC continued to pursue enforcement actions against major technology companies in relation to children's and teens' privacy. For example, the FTC referred a complaint to the DOJ against a technology company for possibly violating COPPA by allowing children to use its application without parental consent. The FTC also took action against an anonymous messaging application marketed to kids and teens for allegedly violating COPPA by failing to ensure that a parent receives direct notice of and consents to its practices around collecting, using, or disclosing their child's personal information.[96] Although not an enforcement action, the FTC additionally examined the data collection and use practices of nine big technology companies, which eventually led to a report upon which the FTC based recommendations to policymakers and companies.

g. Biometric Information

In May 2023, the FTC published its Policy Statement on Biometric Information. See the Biometric Information section of our 2024 annual update for additional details on the policy statement. The policy statement specified that making unsubstantiated marketing claims regarding the validity, reliability, accuracy, performance, fairness, or efficacy of technologies relying on biometric information constitute deceptive practices under Section 5 of the FTC Act. In December 2024, the FTC announced a proposed consent order with an AI and Deep Learning-based video analytics and video cloud software company to settle the FTC's allegations that the company could not substantiate its marketing claims on the accuracy of its facial recognition technologies, including its accuracy across genders, ethnicities and skin tones. The proposed order prohibits the company from making misrepresentations regarding the efficacy and lack of bias in its facial recognition technologies.

2. Consumer Financial Protection Bureau

Over the past year, the CFPB finalized and proposed multiple rulemakings which implicate privacy issues, with a flurry of such action in the waning days of the Biden Administration. As of this report's publication, the Trump Administration has paused implementation of several of these rulemakings, and the agency's future is currently uncertain.

a. A Dramatic Shift Under the Trump Administration

Following significant actions by the CFPB in 2024—including related to data privacy, data security, and algorithmic decisionmaking—thus far in 2025, the interim CFPB Directors appointed by President Trump have imposed significant operational changes that raise significant questions about the agency's future scope and direction. After removing Rohit Chopra as CFPB Director on January 31, 2025, President Trump appointed in quick succession Treasury Secretary Scott Bessent and then Office of Management and Budget Director Russell Vought as Acting CFPB Directors. Bessent and then Vought moved rapidly to freeze virtually all CFPB activities, ordering employees to stop all enforcement and litigation activity; halting rulemakings and suspending effective dates of pending rules; closing the CFPB's Washington, DC office for a week and cancelling the headquarter's lease; canceling the CFPB's next pull of funding from the Federal Reserve; cancelling over $100 million in vendor contracts; firing probationary-period staff; and dismissing (without explanation) various enforcement actions filed during the Biden Administration. While President Trump and the head of DOGE, Elon Musk, have expressed a desire to eliminate the CFPB, the Trump Administration has recently taken the position in court that it only intends to make the agency more "streamlined and efficient." Consistent with this position, Jonathan McKernan, President Trump's nominee for CFPB Director, testified in early March before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, that he would continue to enforce consumer protection laws while advocating for reforms to increase accountability and end the CFPB's "past excesses." At the time of publication, McKernan's nomination is pending confirmation.

b. Impact of the Trump Administration's Actions on the Pre-Trump CFPB's Ambitious Agenda

Precisely how CFPB under Trump-appointed leadership will reshape the agency's approach to consumer protection remains to be seen. The outgoing CFPB pursued an ambitious and aggressive rulemaking, policy, and enforcement agenda, often in reliance

on novel and expansive interpretations of its statutory authority. In the near term, regulated parties can expect new CFPB leadership to critically examine these initiatives—likely rescinding some rules and guidance, and continuing to drop certain enforcement actions while continuing to pursue others. For example, there is substantial uncertainty around the agency's key 2024 rulemakings and guidance related to data privacy, data security, and AI. Specifically, on December 3, 2024, the CFPB proposed a sweeping new rule that would subject data brokers to the Fair Credit Reporting Act, with the goal of limiting the sharing of consumer financial data. On March 5, 2025, the comment period for this rule was extended from March 3, 2025, until April 2, 2025, with the Bureau stating it was doing so in order to give interested persons additional time to consider and submit comments. What new leadership will do with respect to this rule remains to be seen, although it seems unlikely they will embrace it in its proposed form. Additionally, the effective date of the agency's final rule issued in October 2024 under Section 1033 of the Consumer Financial Protection Act (CFPA) requiring certain financial institutions to make data such as account and transaction information available upon request to consumers and authorized third parties has been suspended. The ordered suspension sweeps in all other CFPB final rules that had not gone into effect as of February 3, 2025, like the final rule issued in June 2024 aiming to mitigate AI-driven bias in housing appraisals that was slated to go into effect in approximately June 2025. However, a significant final rule issued in November 2024 establishing the agency's supervisory power over nonbank digital payment providers took effect before then-Acting Director Bessent's February 3, 2025 instruction freezing final rules, so whether action will be taken to rescind the rule remains to be seen. The CFPB's prior leadership had also intensified scrutiny of AI in financial services, issuing guidance and a special edition of its Supervisory Highlights emphasizing compliance obligations, which new CFPB leadership may also rescind. In the longer term, the CFPB's future is uncertain. Courts might step in to limit an administrative shutdown of the agency. The National Treasury Employees Union (NTEU), which represents unionized CFPB employees, brought an action in federal court challenging Vought's stop-work directive, arguing that separation-of-powers principles prevent the Trump Administration from winding down a congressionally authorized agency.[97] The court in that matter ordered a senior CFPB official to testify on March 10, 2025 about the status of the agency's statutorily required activities in connection with NTEU's request for a preliminary injunction to halt mass terminations and other cuts. Additionally, the City of Baltimore and Economic Action Maryland Fund has challenged Vought's attempt to transfer the CFPB's funds to the Federal Reserve, arguing, among other things, that such action violated the Administrative Procedure Act because the agency would be deliberately leaving itself without enough funding to perform its legally mandated duties.[98] A preliminary injunction preventing the funds transfer is in place until March 14, 2025.[99]

c. Other Regulators and Private Litigation: Filling a Potential Enforcement Gap

If the CFPB's activities continue to wane, other regulators may step up their enforcement activities. For example, the FTC, which has concurrent enforcement authority with the CFPB over certain statutes, can police "unfair practices" under the FTC Act and has insight into the CFPB's investigations and enforcement under the agencies' memorandum of understanding. State attorneys general also have broad authority to enforce state consumer protection laws, may enforce the (federal) Consumer Financial Protection Act in their respective jurisdictions under 12 U.S.C. § 5552, and have a "blueprint" for enforcement activity in the form of a report published by the CFPB in January 2025, prior to the leadership transition. State banking departments may also enhance supervisory oversight over non-bank financial institutions in light of any perceived supervisory gap at the federal level. Additionally, private litigants may seize upon regulatory uncertainty to pursue consumer litigation. Businesses that have invested in compliance with recent CFPB mandates must now reassess their strategies in light of shifting federal priorities and the possibility of increased state and private litigation risk. As

the regulatory pendulum swings, staying ahead of both federal and state developments will be critical for businesses seeking to navigate this rapidly evolving environment.

3. Securities and Exchange Commission

The SEC continued its historic levels of enforcement activity in 2024, with a continued emphasis on disclosure and transparency requirements surrounding cybersecurity. The SEC's new cybersecurity disclosure rule for public companies also went into effect in 2024, and numerous companies filed disclosures as required under the rule. In addition, the SEC finalized new cybersecurity disclosure rules for broker-dealers and registered investment advisers.

a. Regulation

Companies begin disclosures of cybersecurity incidents. The SEC's new cyber disclosure rule for public companies, which requires them to publicly disclose material cyber incidents, went into effect in December 2023, and 2024 was the first full year of implementation of the rule.[100] In 2024, approximately 50 public companies filed cybersecurity disclosures on Form 8-K. Many of these disclosures were for non-material impacts. Initially, several companies made non-material disclosures under the new cybersecurity reporting Item 1.05, which was specifically created for disclosures of material cybersecurity incidents. As a result, the Director of the SEC's Division of Corporate Finance issued a statement suggesting that such disclosures were appropriate under Form 8-K Item 8.01, which is for miscellaneous statements, rather than Item 1.05. Due to the strict timing requirements, some companies have made filings under item 1.05, stating that the company could not determine that the impact was material, only to later amend their 8-K filing to state that the company had found the impact to not be material. Notably, fewer than 20% of filings state a material impact. Additionally, on June 24, 2024, the SEC issued five new compliance and disclosure interpretations addressing hypothetical scenarios involving the public company disclosure requirement. Four of these interpretations concern ransomware payment, and provide guidance on how to conduct materiality assessments in scenarios where the company makes such a payment, while the fifth addresses materiality determinations following a series of separate but potentially related incidents. ***SEC adopts data breach notification requirements for additional financial institutions***. On August 2, 2024, a final rule went into effect updating Regulation S–P to require registered investment advisers, transfer agents, and broker-dealers to notify customers within 30 days if their information may have been stolen. Covered institutions have 18 months for larger entities or 24 months for smaller entities[101] from the date of publication in the federal register to comply with the requirements. Key requirements under the new regulation include:

- Covered institutions must implement an incident response program regardless of whether an incident has occurred.
- Covered institutions must disclose an incident to customers as soon as practicable, and no later than 30 days after discovery of an incident. The customer notices must include details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves. This requirement is waived where an institution determines that the affected data will not be used or it is reasonably likely that it will not be used in a way that adversely affects customers.
- Expands existing requirements to safeguard customer data and dispose of unused customer data to include additional types of data and apply to transfer portals in addition to previously covered institutions.

b. Enforcement

Court dismisses much of the SEC's complaint against Software Company. The SEC originally sued a software company in 2023 over a high-profile breach of the company's computer system in 2020. In light of the breach, the SEC alleged that the company had made materially false statements regarding its cybersecurity practices in certain public filings and on its publicly facing website, then subsequently made misleading statements regarding a series of cybersecurity incidents that culminated in a high-profile cyber attack. As we previously discussed in our July 25, 2024 client alert, the court dismissed the majority of the SEC's claims. The remaining claims are related to the Security Statement that the company posted to their website in 2017. Most notably, the court rejected the SEC's attempt to bring an internal accounting controls violation claim under Section 13(b)(2)(B) in the context of cybersecurity-related actions. The court reasoned that the SEC's position that its authority to regulate an issuer's "system of internal accounting controls" includes the authority to regulate cybersecurity controls was "not tenable," and unsupported by the statute, legislative intent, or precedent. The court's decision also calls into question the SEC's ability to rely on claims of inadequate disclosure controls and procedures in similar circumstances, given that the court ruled that a single disclosure failure is insufficient to put the adequacy of a company's disclosure controls and procedures in issue. ***SEC fines transfer agent for alleged failure to protect client funds***. A transfer agent was hacked in 2022 and 2023, resulting in the theft of $6.6 million in client funds. The company recovered about $2.6 million and fully reimbursed clients. The SEC found that the transfer agent had failed to take adequate measures to secure client funds, censured the respondent, issued a cease-and-desist order, and fined the transfer agent for $850,000. ***SEC fines stock exchange operator for allegedly failing to meet disclosure requirements***. The SEC alleged that the parent company of a number of stock exchanges waited several days after learning about a cyberattack to inform compliance and legal officials at the subsidiary exchanges. The SEC took the position that this violated the Regulation Systems Compliance and Integrity (Reg-SCI) by preventing the subsidiary exchanges from making their own timely disclosures to the SEC. The company agreed to pay $10 million to settle the charges but did not admit the allegations. ***SEC settles with marketing firm over alleged disclosure and internal control failures***. The SEC settled with a communications and marketing company for $2.1 million over the company's alleged violation of Section 13(b)(2)(B) of the Securities Exchange Act of 1934 and Exchange Act Rule 13a-15a. The SEC alleged that the company failed to create sufficient internal cybersecurity disclosure controls, which resulted in delayed response to a 2021 ransomware attack. The SEC order notes that data security was critical to the company's business because the company secured sensitive client data. The company settled the allegations following an investigation without admitting fault.

c. SEC Enforcement Outlook for 2025

On October 21, 2024, the SEC Division of Examinations published its annual examination priorities, which include cybersecurity as one of the Division's planned areas of focus in 2025. However, President Trump's nominee to chair the SEC is expected to be more pro-business than the outgoing chair, which may result in less enforcement activity overall. Moreover, Republican members of the Commission, Mark Uyeda and Hester Pierce, have expressed skepticism regarding the SEC's previous efforts regarding cybersecurity, with both issuing dissents against recent cybersecurity enforcement actions. Commissioner Uyeda also previously issued a statement sharply criticizing the 2023 public-company disclosure rules. Nevertheless, the SEC recently announced the reformation of the crypto and cybersecurity division as the Cyber and Emerging Technologies Unit, with a focus on "[r]egulated entities' compliance with cybersecurity rules and regulations," among other

priorities. Accordingly, while we expect the SEC will continue to focus on cybersecurity in 2025, there will likely be lower and less aggressive enforcement activity related to cybersecurity.

4. Department of Health and Human Services and HIPAA

In October 2024, the Department of Health and Human Services (HHS) through its Office for Civil Rights (OCR) announced the launch of a Risk Analysis Initiative to guide health care organizations in conducting thorough evaluations of their cybersecurity practices. The initiative focuses on protecting the confidentiality, integrity, and availability of protected health information to reduce the likelihood of cyber incidents. OCR explained that it "created the Risk Analysis Initiative to increase the number of completed investigations and highlight the need for more attention and better compliance with [HIPAA's] Security Rule," which sets standards for protecting ePHI through administrative, technical, and physical safeguards, requiring businesses to conduct thorough risk assessments, implement and document security measures, and maintain continuous ePHI protections. The Risk Analysis Initiative signals renewed interest in enforcing HIPAA's Security Rule, underscoring the need for covered entities to ensure they are conducting thorough and accurate ePHI-related risk assessments. Relatedly, on December 27, HHS issued a notice of proposed rulemaking aimed at improving HIPAA's Security Rule. The proposed rule would require HIPAA-covered entities and their business associates to bolster existing cybersecurity protections for protected health information, including encrypting protected health information, deploying additional technical controls to shield against malicious software, and requiring multi-factor authentication. In announcing the proposed rule, Deputy Secretary Andrea Palm emphasized the "increasing frequency and sophistication of cyberattacks in the health care sector" that "pose a direct and significant threat to patient safety" and disrupt patient care. The responsibility for finalizing the rule now lies with the Trump administration, which may be more skeptical of implementing new regulations. Specifically, President Trump issued an Executive Order requiring a "Regulatory Freeze Pending Review," directing federal agencies, including the HHS, to "not propose or issue any rule in any matter . . . until a department or agency head appointed or designated by the President . . . reviews and approves the rule." Thus, it is unclear whether the proposed rule will proceed under the new administration.

a. Rulemaking on HIPAA Compliance and Data Breaches

HHS finalized two significant HIPAA rules in 2024. On February 8, OCR finalized a rule updating the Confidentiality of Substance Use Disorder Patient Records regulations to improve coordination among providers by allowing a single consent for treatment, payment, and health care operations, while also permitting de-identified disclosures to public health authorities. The rule strengthens patient protections by aligning enforcement with HIPAA, introducing civil penalties for violations, requiring specific consent for substance use disorder counseling notes, and creating a safe harbor for investigative agencies acting with reasonable diligence before requesting records. OCR finalized another rule on April 26, which modifies the HIPAA Privacy Rule to strengthen protections for reproductive health care by prohibiting the use or disclosure of protected health information to investigate or impose liability on individuals, health care providers, or others involved in lawful reproductive health care. The rule also requires covered entities to obtain signed attestations for specific requests related to reproductive health care and mandates that these entities update their Notice of Privacy Practices to reflect these new privacy protections.

b. Telehealth and Data Security Guidance

HHS released a statement in May 2024, explaining that it will extend COVID-era telehealth and audio-only services beyond 2024, as was planned. As HHS explained, this change was prompted by "changes in patterns of care and higher levels of use of telehealth and audio-only services that can be expected to continue into future benefit years." Thus, any telehealth or audio-only services between patients and qualified health professionals "that is reimbursable under applicable state law and otherwise meets applicable risk adjustment data submission standards may be submitted to issuers' External Data Gathering Environment" servers "for purposes of HHS-operated risk adjustment program for the 2024 benefit year and beyond." In practice, the extension of telehealth and audio-only services beyond 2024 allows insurers to include these services in their risk adjustment data, which helps determine the appropriate reimbursement they receive for covering individuals enrolled in the Affordable Care Act marketplace and Medicaid. Through this policy pronouncement, HHS has signaled its ongoing commitment to and recognition of telehealth's growing role in healthcare delivery.

c. Reproductive and Sexual Health Data

In addition to OCR's final rule strengthening data protections for reproductive health care, discussed above, the FTC also took action to protect individuals' reproductive health data. In April 2024, it finalized an order banning a data broker and its successor from sharing or selling sensitive, precise location data, which the FTC alleged could be used to track visits to "medical and reproductive health clinics and places of worship." In addition to the ban, the order requires the data broker and its successor to develop a program to maintain a comprehensive list of sensitive locations, delete previously collected data unless deidentified or consented to by consumers, and establish privacy programs and safeguards to ensure data is not used for identifying individuals or associating with sensitive locations.

d. HHS Enforcement Actions

HHS made data privacy and cybersecurity a key focus in 2024, ramping up enforcement efforts for HIPAA violations, including actions involving "ransomware, phishing, health information left unsecured on the internet, impermissible access to electronic PHI, reproductive health information impermissibly disclosed, and untimely patient access to PHI." Of note, the HHS reached a sizable settlement involving HIPAA Security Rule violations. In December 2024, HHS announced a $1.19 million penalty against Clearway Pain Solutions Institute for violations of the HIPAA Security Rule "following receipt of a breach report that a former contractor for the company had impermissibly accessed their electronic record system" to "retrieve PHI for use in potential fraudulent Medicare claims." HHS concluded that the contractor had gained impermissible access on three separate occasions, compromising the PHI of over 34,000 individuals. OCR also found that Clearway Pain Solutions Institute failed to conduct a thorough risk analysis of potential vulnerabilities to electronic protected health information (ePHI) and failed to terminate former workforce members' access to ePHI. Reproductive health data breaches have been another priority over the last year. On November 26, 2024, HHS announced a settlement with Holy Redeemer Family Medicine for HIPAA Privacy Rule violations linked with disclosure of a female patient's entire medical record to a prospective employer. The disclosure allegedly included the patient's obstetric and gynecological history, as well as "other sensitive health information concerning reproductive health care." The HHS complaint stated that Holy Redeemer Family Medicine violated the HIPAA privacy rule because it lacked the adequate consent for the release of the full medical record.

Under the settlement, Holy Redeemer Family Medicine agreed to pay a fine and implement a comprehensive corrective action plan requiring it to submit breach notification reports to HHS, develop policies for compliance with the Privacy Rule, and train employees on HIPAA compliance. Lastly, HHS also ramped up enforcement under OCR's Risk Analysis Initiative, announcing its first enforcement action under the initiative in October 2024. A 2022 ransomware attack affected the PHI of 14,273 patients at Bryan County Ambulance Authority (BCAA), prompting OCR's investigation into the entity's alleged failure to conduct a proper risk analysis. HHS found that the entity had failed to conduct a compliant risk analysis to determine the potential risks to its ePHI systems. The parties reached a settlement requiring BCAA to pay $90,000, implement a corrective action plan to ensure HIPAA Security Rule compliance, and submit to a three-year OCR monitoring.

5. Other Federal Agencies

a. Department of Homeland Security

The Department of Homeland Security (DHS), together with the European Commission's Directorate-General for Communications Networks, Content, and Technology, released a joint report comparing cyber incident reporting frameworks, further expanding on its earlier efforts in standardizing reporting processes. By identifying key similarities and differences, the report aims to inform future evaluations of cyber incident reporting processes and enhance alignment between U.S. and EU cybersecurity measures, in particular through a comparative analysis of the recommendations from the U.S. Cyber Incident Reporting Council, the 2023 DHS report on Harmonization of Cyber Incident Reporting to the Federal Government, and the EU's NIS2 Directive (Directive 2022/2555). Further input has also been provided by the Cybersecurity and Infrastructure Security Agency (CISA) and the European Union Agency for Cybersecurity (ENISA). The DHS's CISA has also published several updated guidelines, including an updated "Trusted Internet Connections (TIC) 3.0 Catalog," providing a list of deployable security controls, security capabilities, and best practices, along with multiple updates to its "Public Safety Communications and Cyber Resiliency Toolkit" or the "Marine Transportation System Resilience Assessment Guide." It has recently also published a revised "National Cyber Incident Response Plan," to which stakeholders from across public and private sectors could provide their input by January 15, 2025. Additionally, CISA has been involved in investigations regarding allegations that the People's Republic of China (PRC) targeted commercial telecommunications infrastructure. CISA notified affected companies, rendered technical assistance, and shared information to assist potential victims. Lastly, CISA is also investigating the recent cybersecurity incident at the U.S. Department of the Treasury.

b. Department of Justice

Final Rule on Foreign Adversaries' Access to Sensitive Data. On December 27, 2024, the Department of Justice (DOJ) issued a Final Rule aimed at restricting foreign adversaries' access to Americans' sensitive personal and government-related data. Previously, in February 2024, the Biden administration already directed federal agencies to halt the transfer of sensitive American data to China, Russia, and other foreign adversaries via a corresponding executive order. This Final Rule now grants the DOJ authority to prohibit or impose stringent conditions on transactions involving such data when they pose a national security threat. Among other things, the rule bans transfer of three types of data to parties affiliated with the target countries: (1) bulk U.S. sensitive personal data, which includes covered personal identifiers, precise geolocation data,

biometric identifiers, human genomic data, and personal financial data; (2) U.S. government-related data, which includes any data that is either precise geolocation data for certain locations, or sensitive personal data linked or linkable to certain government employees or contractors; and (3) human genomic or biospecimen data.[102] Additionally, companies handling personally identifiable information, financial data, healthcare records, and biometric data are therefore advised to review their cross-border data transfer agreements and conduct data risk assessments, ensure localization of critical datasets, and implement sufficient contractual protections when dealing with international data partners. In short, this rule requires U.S. companies to be able to identify any transaction that could allow access to covered data by a foreign entity, in particular from China, Cuba, Iran, North Korea, Russia, and Venezuela. ***Children's Privacy Violations***. In August 2024, the DOJ, with urging from the FTC and Congress, filed a civil lawsuit in the U.S. District Court for the Central District of California against a social media company over violations of children's privacy laws. Allegations include unauthorized data collection, application of digital tools to surveil minors, and other non-compliance with COPPA. In particular, according to the complaint, from 2019 to the present the company knowingly permitted children to create regular accounts (i.e., not accounts created in the so-called "Kids Mode") and interact with adults, collected their personal information without parental consent (even for those accounts which were created in Kids Mode), and failed to delete this data upon parental request, while having inadequate policies to manage children's accounts. The complaint further alleges that the company also violated a 2019 Permanent injunction, in part by neglecting its mandate to preserve records about activities from minors below the age of 13 on the platform. ***Civil Cyber-Fraud Initiative***. Initiated in 2021, the DOJ's Civil Cyber-Fraud Initiative (CCFI), which is intended to encourage disclosure and to hold accountable entities and individuals that put U.S. information or information systems at risk by knowingly providing deficient cybersecurity products or services, misrepresenting their cybersecurity practices or protocols, or violating obligations to monitor and report cybersecurity incidents and breaches, gained significant momentum in 2024, leading to multiple settlements with government contractors and private companies accused of failing to meet cybersecurity standards.[103] Such failure to comply can take multiple forms, including outright violations of legal provisions, falsified cybersecurity certificates, or an inability to fulfill contractual obligations. While multiple cases concerning disputes over compliance with federal cybersecurity requirements have been settled, United States ex rel. Craig v. Georgia Tech Research Corp remained ongoing, supported by an intervention from the DOJ in August 2024, at the time of the publication of this article. Companies contracting with the US Government must adhere to National Institute of Standards and Technology (NIST) cybersecurity frameworks to mitigate enforcement risks (also, see below, section A.5.c. Department of Commerce). ***Cybercrime and Dark Web Marketplaces***. The DOJ has intensified efforts to enforce against cybercrimes relating to cryptocurrencies, and dismantle cybercrime marketplaces selling stolen data, hacking tools, or illicit goods. Key operations included the takedowns of the dark web marketplaces Nulled and Cracked (which impacted at least 17 million victims from the United States), and the takedown of Rydox (which sold, amongst others, sensitive data from thousands of victims residing in the United States), along with arrests regarding Incognito Market, an extensive dark web effort to traffic illicit drugs to the United States and around the world. Furthermore, the DOJ, often in collaboration with international partners, also successfully targeted ransomware groups responsible for major cyberattacks, including, amongst others:

- Together with its international partners and the FBI, the DOJ disrupted the LockBit ransomware group, one of the most active ransomware groups in the world that has targeted over 2,000 victims, received more than USD 120 million in ransom payments, and made ransom demands totaling hundreds of millions of dollars. Actions against LockBit included seizing numerous websites and servers managed by LockBit administrators. These were complemented by indictments against key figures, the issuing of the search warrants, and the development of decryption capabilities to restore systems encrypted by the LockBit ransomware variant.
- An alleged North Korean government-affiliated cybercriminal was charged for

attacks targeting U.S. hospitals and critical infrastructure.

c. Department of Commerce

In October 2024, the U.S. Department of Commerce (DOC), through the Bureau of Industry and Security's (BIS) Office of Information and Communications Technology and Services (OICTS), issued a landmark decision prohibiting the use of Kaspersky's antivirus software and cybersecurity products in the United States or by U.S. persons, "*due to the Russian Government's offensive cyber capabilities and capacity to influence or direct Kaspersky's operations*." The decision marked the first time OICTS exercised its authority with regards to Information and Communications Technology and Services (ICTS) supply chain regulations. While it was based on an interim final rule implementing an Executive Order from the Biden administration, the corresponding final rule was issued in December 2024. Additionally, cybersecurity risks stemming from supply chains have in particular been under heightened scrutiny of the DOC—although the impact of the new Trump administration on these remains to be seen:

- For example, the BIS issued a Notice of Proposed Rulemaking regarding a rule banning the import and sale of connected vehicles from China (including Hong Kong) and Russia, citing risks related to espionage, cyber threats, and unauthorized data collection, which has been finalized while still under the Biden administration on 19 January 2025. The rule also restricts key vehicle software and hardware deemed to pose "undue or unacceptable risks" to national security, with certain software restrictions beginning in 2027 and hardware restrictions following in 2029.
- Furthermore, BIS has announced an Export Control Framework to further strengthen the U.S.'s cybersecurity capabilities from a hardware perspective. The framework is aimed at limiting the spread of advanced artificial intelligence technologies while tightening restrictions on advanced computing. It specifically imposes strict controls on the export, reexport, and transfer of advanced computing integrated circuits and the model weights of leading AI systems.
- BIS has also proposed a new rule imposing restrictions on U.S. Infrastructure-as-a-Service (IaaS) providers, in particular cloud service providers, concerning their role in training large AI models. The rule would require IaaS providers to implement Customer Identification Programs (CIPs) to collect "Know Your Customer" (KYC) information, and is ultimately aimed at preventing foreign adversaries from accessing advanced AI capabilities.

Separately, in February 2024, the DOC's National Institute of Standards and Technology (NIST) released Version 2.0 of its Cybersecurity Framework (CSF). The updated CSF is now organized around six key functions: Identify, Protect, Detect, Respond, and Recover, along with CSF 2.0's newly added "*Govern*" function, emphasizing the importance of cybersecurity governance and risk management. It also now addresses explicitly all organizations and not just those in critical infrastructure, its original target audience. Lastly, in December 2024, the DOC released a strategic report titled "*The Decisive Decade: Advancing National Security at the Department of Commerce*." The report outlines key policy objectives in the digital space, emphasizing U.S. leadership in critical technologies, international security collaborations, and private-sector partnerships to enhance cybersecurity. It serves as a roadmap for maintaining economic security and technological dominance while addressing threats from foreign adversaries.

d. Department of Energy

Cybersecurity continues to be a point of emphasis underpinning power systems and critical infrastructure resilience. In 2024, the U.S. Department of Energy (DOE) released and endorsed various implementation strategies and adoption guidelines intended to drive the voluntary adoption of uniform cybersecurity practices across the energy sector. In March 2024, the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) partnered with the National Association of Regulatory Utility Commissions (NARUC) to publish "Cybersecurity Baselines" for distributed energy resources (DERs) and their electric distribution systems. Intended for asset scoping and baseline prioritization, the Cybersecurity Baselines are intended to enhance system resilience and provide a starting point from which a solid cybersecurity foundation can be built and later expanded upon, following a risk-informed roadmap. The final version of the accompanying Implementation Guidance is expected to be published in mid-2025. Cybersecurity also remains a critical pillar of DOE's efforts to protect clean energy infrastructure. In particular, a key focus has been modernizing and securing U.S. hydropower plants, which is central to the DOE's cybersecurity strategy. The DOE has also issued several cybersecurity guidelines, including those for energy procurement and introduced new Supply Chain Cybersecurity Principles, developed in collaboration with Idaho National Laboratory. In addition, the Energy Threat Analysis Center (ETAC)—a public-private partnership that convenes experts from the federal government and the U.S. energy sector—became operational in Q4 2024. Jointly managed by CESER and the DOE's Office of Intelligence and Counterintelligence, and in partnership with the national laboratories, and in close coordination with the Cybersecurity and Infrastructure Security Agency (CISA) Joint Cyber Defense Collaborative (JCDC), it is aimed at strengthening the collective defense, response, and resilience of the U.S. energy sector, improve national security in the energy sector, enhance analysis capabilities and facilitate an increased sharing of information. In addition to providing external guidance and support, the DOE has also continued efforts to enhance its own cybersecurity following recent cyberattacks. In particular, in January 2024, the DOE issued its Cybersecurity Strategy. Other governmental bodies also highlighted the importance of the DOE and its mission to protect sensitive data and critical infrastructure as well as ensuring supply chain security. For example, the Office of the Inspector General (OIG) noted that a crucial role for this will fall on the recently established Vetting Center, where a Vetting Center Policy Group has been established in 2024. Assessing the outcome of this will be crucial for contractors and vendors doing business with the DOE, as they should anticipate increased emphasis on and scrutiny of their cybersecurity practices in 2025.

e. Department of Defense

In October 2024, the Department of Defense (DoD) finalized a much anticipated rule implementing its Cybersecurity Maturity Model Certification (CMMC) program for defense contractors, broadly aimed at increasing the security of controlled, unclassified information within the defense industry.[104] The CMMC will set three "levels" of cybersecurity requirements based on the nature of information held by contractors, with the aim of creating a baseline level of cybersecurity for almost all DoD contract solicitations. These requirements include confirming that Cloud Service Providers used by contractors meet certain risk standards, protocol for processing, storing, and transmitting controlled unclassified information; and submitting annual compliance self-assessments. In addition to enhancing the cybersecurity of its supply chain, the DoD announced its plan to prioritize strengthening its Defense Industrial Base (DIB), which is a network of foreign companies and organizations that support the DoD and other U.S. defense requirements. In March 2024, the DoD announced a cybersecurity strategy aimed at improving the DIB's cybersecurity capabilities and its IT interoperability and integration with the DoD, and in May 2024, the DoD's Chief Information Officer released a playbook for implementing shared security authorization packages across DoD systems to make system assessments more efficient. In June 2024, the Pentagon released a blueprint for the DoD to prioritize providing joint warfighting IT capabilities between U.S. forces and mission

partners, modernizing information networks, optimizing IT governance, and cultivating a digital workforce.

f. Federal Communications Commission

As noted in the 2023 update, the Federal Communications Commission (FCC) announced its new Privacy and Data Protection Task Force in June 2023. Since its inception, the Task Force has been active in various enforcement and rule-making efforts. ***Enforcement***. The FCC also levied large fines and settled several claims related to company data practices. In April 2024, the FCC fined American wireless carriers nearly $200 million for allegedly sharing their customers' location data without consent. The FCC Enforcement Bureau investigation found that the carriers sold location data access to aggregators, who then resold the access to third parties, in an alleged attempt to offload their obligation to obtain customer consent. In June 2024, a leading Latin American telecommunications company agreed to pay $100,000 to resolve allegations that the company failed to report a data breach in a timely manner in violation of FCC rules and conditions of Liberty's license. In July 2024, the FCC announced a $34.6 million settlement and consent decree with a phone captioning company to resolve allegations that the company unlawfully retained call content beyond the duration allowed and submitted inaccurate information to the Telecommunications Relay Service (TRS) Fund Administrator. Also in July 2024, the FCC announced a $16 million settlement with an American wireless prepaid service provider to resolve allegations that the company failed to reasonably protect customer information in connection with multiple data breaches. In September 2024, a major American wireless carrier entered into a $13 million settlement with the FCC regarding a data breach of a cloud vendor for the carrier, exposing customer information that the vendor was supposed to have destroyed. The FCC faulted the carrier for failing to ensure the vendor had destroyed the data. Also in September 2024, another major American wireless carrier reached a $31.5 million settlement with the FCC to resolve investigations into multiple data breaches, including access to the names, addresses, dates of birth, and Social Security numbers for 47.8 current, former, and prospective customers. The $31.5 million settlement consisted of a $15.75 million penalty and a $15.75 million investment by the carrier into its cybersecurity infrastructure. ***TCPA Rulemaking***. The FCC continued its focus on curtailing robocalls and robotexts by adopting new rules in February 2024. While previous rules have made it clear that consumers have a right to revoke their consent to receive automated calls and messages, the new rules require that revocation requests be honored within a reasonable time, not to exceed 10 business days from receipt. The rules also codified the FCC's previous ruling that consumers can revoke their consent through any reasonable means. Approved in December 2023, TCPA rules requiring lead generators, comparison shopping websites, and similar companies to obtain a consumer's prior express written consent to receive automated calls from each marketing partner went into effect on January 25, 2025.[105] A February 3, 2025 decision from the Eleventh Circuit Court of Appeals recently vacated this "one-to-one consent rule" under the TCPA, which may create uncertainty for other recent TCPA regulations.[106] ***Cyber Trust Mark***. In March 2024, the FCC voted to create a voluntary cybersecurity labeling program for devices that meet certain cybersecurity and privacy standards. Qualifying products will bear a label including a new "U.S. Cyber Trust Mark" to help consumers differentiate trustworthy products and will also include a scannable QR code with additional product information. Examples of eligible products include smart home appliances and fitness trackers.

6. State Agencies

State attorneys general continued to lead the charge as privacy regulators in 2024, enforcing both existing consumer protection laws and comprehensive data privacy laws that an increasing number of states are enacting. Attorneys general have not been alone

in their work, however, as other state agencies, including new dedicated privacy regulatory agencies, work in tandem with attorneys general. State agencies and state attorneys general are expected to be particularly active and continue the trend in 2025 in light of the Trump administration's predicted reduction in enforcement activity at the federal level.

a. California

i. California Privacy Protection Agency

In 2024, the California Privacy Protection Agency (CPPA) began to take a more active role in privacy regulation and enforcement in California. In January 2024, the agency launched a website dedicated to enlightening the public regarding privacy rights and, throughout the year, announced partnerships and initiatives related to strengthening privacy protections. The CPPA also published its first two California Consumer Privacy Act (CCPA) enforcement advisories, addressing the application of data minimization to consumer requests and avoidance of dark patterns, respectively. Along with the enforcement advisories, the CPPA and AG have issued confidential notices of violation to various companies, including, but not limited to the scope of their enforcement advisories. Additionally, the CPPA announced changes to its leadership. After over three years leading the CPPA, Executive Director Ashkan Soltani stepped down from his position, effective January 2025. Tiffany Garcia, the former Chief Deputy Executive Director of the CPPA, will serve as Interim Executive Director until a permanent replacement is named. Before joining the CPPA, Garcia served for four years as Deputy Secretary for Fiscal Policy and Administration at the California Business, Consumer Services and Housing Agency. On January 1, 2024, the California Department of Justice transferred administrative responsibility for the state's data broker registry to the CPPA. In October 2024, the CPPA announced a public investigative sweep of data broker registration compliance. The CPPA subsequently announced a series of settlement agreements with data brokers resolving claims that the companies failed to register and pay required fees, which is subject to a $200 fine per day. In December 2024, the CPPA voted to adopt regulations substantially increasing the fees for data broker registration from $400 to $6,600 and clarifying procedural requirements under California's Delete Act, which requires data brokers to register with the CPPA. In November, the CPPA advanced draft CCPA regulations on cybersecurity audits, risk assessments, and automated decisionmaking technology (ADMT) to the formal rulemaking process. The notice and comment period was open from November 22, 2024 until February 19, 2025. In addition to adding rights and requirements for the use of ADMT (described in detail in the), the proposed regulations would revise the existing CCPA regulations to require businesses to conduct cybersecurity audits and risk assessments. These changes include an expansion of the definition of sensitive personal information, additional requirements for implementing consumer rights, and updates to the opt-out framework. Gibson Dunn has laying out the significant issues with the draft regulations.

ii. California Attorney General

Though the CPPA has begun privacy enforcement in California, the California Attorney General (CA AG) continued to play an active role in enforcing the CCPA in 2024. In January 2024, the CA AG announced an investigative sweep focused on streaming

services. The CA AG also announced two settlement agreements under the CCPA in 2024. The first, with a major tech company, handled by Gibson Dunn, addressed the CCPA's requirement that a business disclose and provide consumers the right to opt out of the selling or sharing of their personal information. The settlement agreement required a low settlement penalty of $375,000 and injunctive terms that reiterated existing requirements of the law but notably did not require any changes to business practices. The second settlement, which the CA AG brought with the Los Angeles City Attorney, resolved claims that a mobile game company violated the CCPA and COPPA by failing to obtain parental consent for collecting and sharing children's data from a mobile app. In addition to a $500,000 civil penalty, the settlement agreement requires the company to obtain consent for processing children's and teen's personal information, provide a just-in-time notice when children's data is sold or shared, and properly configure third-party software-development kits to comply with children's data legal requirements.

b. Other State Agencies

In 2024, state attorneys general in other states began to enforce their recently enacted state comprehensive privacy laws and build out privacy enforcement infrastructure. For example:

- The Texas Attorney General (Texas AG) has been particularly active in enforcing Texas's data protection laws. In June 2024, the Texas AG announced the launch of a data privacy and security initiative, establishing a dedicated data privacy protection team. Focused on the sale of geolocation data, the Texas AG opened an investigation into car manufacturers' collection and sale of driver data and subsequently brought a lawsuit against a car manufacturer under the Deceptive Trade Practices Act. The Texas AG issued notices of violation to multiple other companies for allegedly sharing sensitive user data without proper notice and consent under the recently effective Texas Data Privacy and Security Act and notifications of apparent failure to register as data brokers to over 100 companies a few months after the close of the Texas Data Broker Law's initial registration period . Gibson Dunn has advised clients in response to many confidential investigations and notices over the past year. The Texas AG also filed a complaint against a popular social media platform under the SCOPE Act, alleging that the company failed to obtain parental consent before sharing, disclosing, or selling a minor's personal information and failed to offer required parental controls.
- In February 2024, the Connecticut Attorney General (CT AG) published a report describing enforcement actions under the Connecticut Data Privacy Act in the first six months since the law took effect. The report states that the CT AG has issued numerous warning letters, received 30 complaints, issued inquiries and cure notices addressing deficiencies in privacy policies, sensitive data, teen data, and data brokers.
- In December 2024, the Colorado Department of Law adopted rules updating language in the Colorado Privacy Act Regulations to include newly adopted definitions of biometrics and adding a process for issuing opinions and guidance. Additionally, as part of a roll-out process, the Colorado Attorney General recognized Global Privacy Control (GPC) as the first universal opt-out mechanism to meet the CPA's standards, and required businesses to implement GPC opt-outs by July 2024.
- The Oregon and Virginia Attorneys General have initiated confidential investigations into compliance with their newly effective state privacy laws, some of which have been handled by Gibson Dunn.
- Ahead of the January 1, 2025 effective date of the New Hampshire Data Privacy Act, the New Hampshire Department of Justice announced the creation of a data

privacy unit. Delaware created a Personal Data Privacy Portal in anticipation of the Delaware Personal Data Privacy Act, which also took effect January 1, 2025.

III. Civil Litigation Regarding Privacy and Data Security

A. Data Breach Litigation

Data breaches and cybersecurity incidents have continued to pose a threat to businesses, resulting in substantial economic losses and putting companies at risk of litigation. According to the Identity Theft Research Center (ITRC), although there were fewer data breaches in 2024 than in 2023—2,850 as opposed to 3,122 total data breaches—due to the scale of some of the 2024 breaches, the number of data breach victims actually increased by 257% from 2023. We summarize a few of the notable data breach suits below. A large telecommunications company faced multiple class action lawsuits stemming from a data breach that allegedly resulted in the exposure of approximately 73 million account holders' personal data.[107] These class actions have now been transferred to and consolidated in the Northern District of Texas, alleging claims for, among other things, negligence, breach of contract, and unjust enrichment.[108] The class actions also allege that the telecommunications company violated state consumer protection laws, deceptive and unfair trade practices laws, and personal consumer information laws.[109] A federal court denied a pharmaceutical wholesaler's motion to dismiss, finding that plaintiffs had adequately pleaded standing in seeking damages for the risk of future harm resulting from a data breach.[110] Specifically, the court found that, because the plaintiff had pleaded actual attempted misuse, standing had been adequately pleaded, even though the attempted misuse was prevented by the Social Security Administration.[111] A pair of recent decisions also provide insight into the role that fiduciary duty claims play in data breach litigation. In November 2024, the Supreme Court of Alabama affirmed a lower court dismissal of a data breach class action against a management consulting firm, which had allegedly collected sensitive personal and health information from employees, patients, and vendors; and where the submission of sensitive personal information is a pre-requisite for employment.[112] The court affirmed the dismissal of the case due to lack of standing and failure to sufficiently plead claims, including because the plaintiff failed to plead that a fiduciary duty existed between her and her former employer.[113] Specifically, the court held that while Griggs argued that as NHS has influence and dominion over Griggs and her data, under Alabama precedent, a principal or employer is not the fiduciary of the agent or employee, and Griggs failed to provide any support for the court to provide an exception in her case. In a July 2024 decision out of the Northern District of Georgia, a court found that a plaintiff had sufficiently pleaded evidence to show a fiduciary relationship existed between a company that retained health information.[114] Unlike the Alabama case, the Georgia case did not involve an employer-employee relationship. The Northern District of Georgia court allowed breach of fiduciary duty claims, determining that "in some circumstances, the retention of private information that patients provided while seeking medical care can create a fiduciary duty under Georgia law."[115] Additionally, 2024 saw a number of significant data breach settlements that will shape what new cases are filed and negotiation in existing cases:

- A health network agreed to a $65 million settlement, which was later approved by the court, to resolve the claims of nearly 135,000 patients and employees whose personal data was breached due to a ransomware attack, including more than 600 patients who had their personal medical-record photos posted on the internet after the health network refused to pay the ransom.
- A personal genomics company agreed to a $30 million settlement to resolve a multi-district class action brought on behalf of more than six million customers who claimed that their personal data was stolen, including, for a small set of customers, information about their health based on the analysis of their genetic data.
- A mobile payment company and its subsidiary agreed to a $15 million settlement to settle claims stemming from two separate data breaches, one by a former employee and another by third parties that used old phone numbers to access

users' accounts, that allegedly exposed the personally identifiable information, account numbers, and trading activity of more than 8.2 million users.

B. Wiretapping and Related Litigation Concerning Online "Tracking" Technologies

The flood of lawsuits brought under federal and state wiretapping statutes continued in 2024, with hundreds of cases being filed, frequently by the same plaintiff law firms. Many technology companies offer web- and app-based tools (such as software development kits, pixels, chat features, or similar tools) that web and app developers can use to track users' activity on their website or app. Plaintiffs have brought lawsuits alleging that the use of these tools in a variety of different sectors (such as healthcare, video, finance, and more) violates federal and state wiretapping statutes by "recording" (or "eavesdropping" on) plaintiffs' activity on websites and apps (which plaintiffs characterize as their "communications" with web and app developers). For example, plaintiffs have alleged that third-party technology companies were able to "wiretap" and "eavesdrop" on their online chat communications with businesses through the technology used to implement those chat features.[116] Some of these lawsuits were filed directly against the developers that own the websites and apps at issue.[117] Others were filed against the companies that offer this technology to web and app developers and allegedly receive the communications at-issue.[118] As described in last year's Review, the plaintiffs in these cases often bring claims under both the federal Wiretap Act and state wiretapping laws, which can carry high penalties for violations. The federal Wiretap Act is a one-party consent statute, so there is no liability if even one party to a communication consents to share it unless the communication is intercepted for the purpose of committing a crime or tortious act.[119] The Act provides for statutory damages consisting of $100 a day for each day of violation or $10,000, whichever is greater.[120] Some states have adopted more restrictive two-party (or all-party) consent statutes while also providing for high statutory damages. For example, California's wiretapping and eavesdropping laws prohibit wiretapping or eavesdropping on communications without the consent of all parties involved and provide for $5,000 in statutory damages per violation.[121] These claims continue to be especially difficult to defend against at early stages of the case, as courts in 2024 have sometimes refused to consider a defendant's privacy policy to show consent at the motion-to-dismiss stage.[122] A significant number of these cases have continued to survive past the pleadings stage, though several others have been dismissed outright.[123] In one significant decision, a California federal district court dismissed wiretapping and other privacy-based claims against a technology company **based on the plaintiffs' failure to plausibly allege that the company intended for third parties to use its pixel technology to send sensitive health information** (contrary to the company's instructions).[124] This decision teed up an intra-District split on the proper standard for assessing intent for wiretapping claims in the Northern District of California, where many of these cases are brought.[125] In addition, the caselaw has continued to develop regarding what sort of harm plaintiffs must show to pursue a claim, with some courts finding a statutory violation sufficient (based on an asserted privacy injury)[126] and others requiring more in light of a 2021 U.S. Supreme Court decision.[127] There were more decisions in 2024 at the summary judgment stage as well, with mixed results. For example, a California federal court granted summary judgment for the defendant web developer on the plaintiff's California wiretapping claim.[128] The plaintiff alleged the defendant violated California's wiretapping statute when she visited the defendant's website, because her keystrokes were recorded by computer code embedded on the website.[129] The plaintiff claimed that this recording violated the California wiretapping statute's prohibition on "read[ing] or attempt[ing] to read or learn the contents or meaning of electronic communications" without the consent of all parties to the communication.[130] The court held the defendant did not "read, attempt to read, or to learn the contents or meaning" of the communications because the keystrokes were immediately "hashed," or transformed into an "incomprehensible alphanumeric string called a hash," and the unhashed information was not retained anywhere.[131] As another example, another California federal court granted summary judgment for the defendant social media companies on the plaintiffs' federal and California wiretapping claims.[132] The plaintiffs alleged the

defendants' web-based tools collected and sent their information when they visited websites that used those tools.[133] The court held plaintiffs had not produced any evidence that the defendants had intercepted the "contents" of their communications as required under the federal and California wiretapping claims, and that even if plaintiffs had done so, it did not appear the defendants had obtained any communications "during transmission" as to one of the two tools.[134] By contrast, another California federal court denied in substantial part a technology company's motion for summary judgment in a lawsuit where the plaintiffs alleged their private health information entered into a period-tracking app was surreptitiously shared with the technology company through the company's software development kit embedded on the app.[135] The court permitted the plaintiffs' federal and California wiretapping claims to proceed, finding "factual disputes" existed regarding "the alleged transmission of data via [the defendant]'s SDK, and its subsequent use vel non."[136] In 2024, certain tracking technology cases also reached preliminary or final settlements encompassing wiretapping claims. For example, the plaintiffs filed an unopposed motion for final approval of the parties' proposed class action settlement in a case based on a technology company's purported surreptitious tracking of users' web-browsing activity even when users browsed in "Incognito mode."[137] Included as part of this "groundbreaking settlement that yields substantial benefits" for class members are the technology company's agreements to rewrite its disclosures to inform users that it collects private browsing data, to "delete and/or remediate billions of data records that reflect class members' private browsing activities," and to permit users in Incognito mode to block third-party cookies by default.[138] Under the terms of the settlement, class members retain their right to sue the defendant individually for damages, including for the "significant statutory damages available under the federal and state wiretap statutes."[139]

C. Anti-Hacking and Computer Intrusion Statutes

The federal Computer Fraud and Abuse Act (CFAA) generally makes it unlawful to "intentionally access a computer without authorization" or to "exceed[] authorized access."[140] As described in last year's Review, the U.S. Supreme Court's decision in *Van Buren v. United States*, 593 U.S. 374 (2021), subsequent cases, and the Department of Justice's decision in 2022 to narrow its CFAA enforcement policies have limited the CFAA's legal and practical scope. Decisions this past year have continued to grapple with the proper scope of the CFAA and similar state statutes, such as California's Comprehensive Data Access and Fraud Act (CDAFA).

1. CFAA

In 2024, courts continued to confront questions about the scope of "authorization" under the CFAA. For example, in July 2024, a federal jury in Delaware found that an online travel agency violated the CFAA by using an airline's website without authorization or in excess of its authorized access.[141] The airline characterized the travel agency's unauthorized use of its website as "screen scraping," which the airline defined as "using an 'automated system or software . . . to extract data from [the airline's] website for commercial purposes,' such as selling [the airline's] flights on websites other than [the airline]'s."[142] According to the airline, the travel agency continued screen scraping even after the airline sent cease-and-desist letters and developed a program to block such unauthorized activity.[143] The jury awarded $5,000 to the airline, which represented the amount of "actual economic harm" caused by the travel agency's violation of the CFAA.[144] Following the jury verdict, the travel agency filed a motion for judgment as a matter of law, arguing in part that the airline failed to prove that it suffered a loss of at least $5,000 in any one-year period, as required under the CFAA.[145] The court agreed, granting judgment in favor of the travel agency.[146] The court entered an amended judgment in accordance with its ruling on January 31, 2025.[147] This was one of the first civil trials involving a CFAA claim. Other 2024 decisions similarly addressed the meaning of "authorization" under the statute. In a case before the Sixth Circuit, an IT administrator created company email accounts for potential buyers of the company to use.[148] When

the potential purchase fell through, the IT administrator searched the buyers' email accounts to preserve certain emails for litigation purposes.[149] The Sixth Circuit held that the IT administrator's actions were not "without authorization" because, as the manager of the email accounts, he had undisputed authorization to access them.[150] The Sixth Circuit next considered whether the IT administrator's actions "exceed[ed] authorization," observing that "[d]etermining the parameters of authorization . . . is not always easy to pin down."[151] But the court ultimately did not decide the issue, finding the IT administrator did not violate the statute because the CFAA prohibits only "intentionally" exceeding unauthorized access, and the administrator "lack[ed] notice that his access [was] unauthorized."[152] The Sixth Circuit thus affirmed summary judgment in favor of the defendants. As another example, in a federal Idaho case, a company alleged that three of its former employees improperly accessed its internal healthcare record system to obtain confidential and proprietary information to form a competing business.[153] While they were employed by the company, the three defendants were all issued credentials to access the system.[154] After one defendant was fired, he allegedly increased another defendant's permissions in the system, which the latter defendant used to access material he was not otherwise authorized to access. The court pointed to *Van Buren v. United States*, 593 U.S. 374 (2021), noting the Supreme Court had indicated "the question of authorized access is a 'gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.'"[155] The court went on to note that the Supreme Court "left open the issue of 'whether [the authorization] inquiry turns only on technology (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies.'"[156] Because one defendant had allegedly wrongfully expanded the other defendant's access beyond what was authorized, the court held it could not conclude at the motion-to-dismiss stage that such conduct fell outside the scope of the CFAA.

2. CDAFA

Courts have also grappled with issues under state-law analogs to the CFAA, which plaintiffs sometimes invoke alongside wiretapping and other privacy-related claims. One such statute, the CDAFA, is California's version of the CFAA, and its provisions "generally prohibit[] tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems."[157] The CDAFA creates a private right of action against any person who commits certain listed violations "for compensatory damages and injunctive relief or other equitable relief."[158] "Access" under the statute means to "cause output from" the "logical, arithmetical, or memory function resources of a computer."[159] Only someone who has "suffer[ed] damage or loss by reason of a violation" of the statute may bring a civil action.[160] As was the case last year, in 2024, several district courts considered CDAFA claims as part of the recent wave of litigation related to website tracking technologies. Of particular note is what appears to be a growing divide among the district courts on the issue of whether the loss of value in a plaintiff's data can qualify as "damage or loss" under the statute. Most courts have held that the loss of value of personal data is not enough to show "damage or loss" under the CDAFA.[161] For example, a California district court dismissed the plaintiffs' CDAFA claim in a case where the plaintiff alleged her interactions with her medical center's online patient portal, including her private medical data, were surreptitiously forwarded to certain third parties due to the center's use of tracking pixels on its website.[162] The plaintiff argued the loss of value of her data constituted "damage or loss" under the CDAFA. The court rejected that argument, holding that the "loss of the right to control [one's] data, the loss of the value of [one's] data, and the loss of the right to protection of the data" are not losses covered by the CDAFA.[163] Some courts, however, have accepted the lost-value-of-data theory. For example, in a federal California case, the plaintiff alleged that his personal information entered into a chat feature on the defendant's website was surreptitiously shared with other companies due to the code used to support the chat feature.[164] The court declined to dismiss the plaintiff's CDAFA claim, holding the plaintiff had sufficiently alleged that the defendant "has a stake in the value of his misappropriated data."[165] The court pointed to the Ninth Circuit's decision in *In re*

Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020), for support, reasoning that the Ninth Circuit had found the plaintiffs in that case "had sufficiently alleged their [data] carried financial value" under the CDAFA.[166]

D. Telephone Consumer Protection Act Litigation

Originally enacted in 1991, the Telephone Consumer Protection Act (TCPA) regulates certain forms of telemarketing activities and the use of automatic telephone dialing systems (ATDS).[167] TCPA litigation historically centered on issues concerning the technical definition of an ATDS, but in 2021, the Supreme Court clarified and restricted the definition in its 2021 opinion in *Facebook Inc. v. Duguid*, in which the Court endorsed a narrow definition that limited the definition of ATDS to devices that store or produce telephone numbers by using a random or sequential number generator.[168] With the definition of an ATDS largely resolved, the interpretation of other key provisions in the TCPA has become the focus of ongoing litigation. In one notable decision in 2024, the Fourth Circuit reversed a motion to dismiss a putative class action, holding that the plaintiff alleged facts sufficient to state a claim that the defendant's fax invitation to attend a free webinar constituted an "unsolicited advertisement" under the TCPA.[169] The court held that it is reasonable to infer that the free webinar had a "commercial character," even though specific products were not mentioned in the fax.[170] The court further reasoned that, by accepting the defendant's fax invitation, the plaintiff would have potentially provided contact information and consent to future promotional materials—which gave the fax the requisite "commercial nexus" to the defendant's business.[171] On the other hand, the Fourth Circuit held in a different case that the TCPA does not apply to faxes that are received through online fax services.[172] The court reasoned that because an online fax service does not receive an electronic signal "over a regular telephone line" or have the capacity to transcribe text or images "onto paper," it does not meet the statute's definition of a "telephone facsimile machine."[173] Looking ahead, the Supreme Court is expected to issue a decision in a case that addresses whether the Hobbs Act, which limits the judicial review of FCC final orders to appellate courts, requires a federal district court to accept the FCC's interpretations of the TCPA.[174] Because the FCC's interpretations can affect how courts evaluate claims and defenses in TCPA actions, this decision could have a significant impact on how these cases are litigated and resolved.

E. State Law Litigation

1. California Consumer Privacy Act Litigation

The CCPA provides a limited private right of action, allowing consumers, individually and as a class, to pursue civil litigation when their personal information falls subject to "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."[175] The CCPA provides for the greater of either statutory damages—between $100 and $750 per consumer per incident—or actual damages, plus injunctive or declaratory relief, and any other relief a court deems appropriate.[176] In practice, this private right of action is used almost exclusively to address data breaches. While there was not significant movement in 2024 on these issues, some courts have issued rulings supporting an expansive interpretation of what constitutes a "data breach" subject to the private right of action. Moreover, in 2024, several courts focused on the threshold consideration of whether defendants qualified as a "business" subject to the CCPA, as well as defenses to the CCPA. The details of these rulings are summarized below.

a. Limited Reach of the CCPA's Private Right of Action

In several suits over the past year, courts did not reach the merits of alleged violations of

the CCPA because they first assessed whether a defendant was subject to the private right of action. Courts generally interpreted the statute to require that the defendant qualify as a "business"—an entity that collected or otherwise made determinations about how to process plaintiffs' personal data—to be subject to the statute's private right of action, though they differed on whether a traditional service provider could be sufficiently subject to those requirements.[177] For example, in a putative class action against a debt collection and accounts receivable management company, the court dismissed the CCPA claim, holding that though plaintiffs did plead that the company "obtained" and "received" the plaintiffs' PII, the complaint did not allege that the defendant "determined how and why [plaintiffs'] PII should be processed."[178] In another suit, the court held that a cloud-based software company did not qualify as a "business" because enabling the secure transfer of files by hosting them on the company's file-sharing software did not amount to "determin[ing] why and how consumers' PII was processed."[179] However, in a suit against a health information technology company, the court held that the defendant's use of plaintiffs' PII "to develop, improve, and test" the defendant's services—a common type of processing by "service providers"—was sufficient to make it subject to the CCPA.[180] Another court addressed the scope of a data breach, effectively doubling down on prior courts' broadening of the common understanding of the triggering event required for the private right of action. In that case, plaintiffs brought a putative class action against a mental healthcare company that was alleged to have been disclosing users' mental health information to a third party without providing notice to users.[181] The company moved to dismiss the plaintiffs' CCPA claim, arguing that CCPA's private right of action applies only to traditional data breaches.[182] The court disagreed and denied the motion to dismiss the claim, holding that courts have allowed CCPA claims to "survive a motion to dismiss where a plaintiff alleges that defendants disclosed plaintiff's personal information without his consent due to the business's failure to maintain reasonable security practices."[183]

b. Other CCPA Defenses

In 2024, defendants continued to invoke CCPA defenses, such as narrow exemptions and the statute's notice requirement, with varying success. ***International Law Firm***. After an international law firm discovered a significant cybersecurity breach of its systems, plaintiffs brought a putative class action lawsuit against the firm asserting multiple claims, including violations of the CCPA.[184] The firm argued in part in its motion to dismiss that because the named plaintiff was employed by one of the defendant's clients, the "business-to-business" exception applied because the defendant received his data as part of a business-to-business transaction.[185] Though this exemption expired on January 1, 2023, it was in place at the time of the 2021 data breach, so the court dismissed the plaintiff's claim with prejudice.[186] Though defendants can no longer rely on this exemption for data breaches taking place in 2023 and beyond, this case serves as a reminder that it remains a viable defense to breaches occurring before that time. ***Hotel and Casino Entity***. A hotel and casino entity was subject to a data breach in November 2022, in which the PII of thousands of customers was accessed by hackers.[187] A class action suit was brought against the entity asserting multiple claims, including violations of the CCPA.[188] The entity contended plaintiffs' claim for statutory damages under the CCPA was barred because notice of the CCPA claim was untimely.[189] One of the named plaintiffs had filed his individual complaint—which did not assert a CCPA claim—and mailed a CCPA pre-suit notice on the same day.[190] Several months later, plaintiffs filed a consolidated complaint which included a statutory damages CCPA claim.[191] The court held that the plaintiffs had satisfied the notice requirement because the defendant was provided with the required cure period before the plaintiff brought the claim to court.[192] The court further held that the allegations in plaintiff's letter were sufficient to provide statutory notice and that the defendant's measures taken after receipt of the letter did not cure the unauthorized release of the plaintiffs' data and were instead designed to address future threats.[193]

2. State Biometric Information Litigation

a. Illinois Biometric Information Privacy Act (BIPA)

2024 was another active year for Illinois's Biometric Information Privacy Act (BIPA). There were both plaintiff- and defense-friendly developments, as well as a novel, significant settlement. Of note for plaintiff-friendly developments, courts permitted a complaint against a cloud service provider to survive a motion to dismiss, and concluded that plaintiffs located outside Illinois may be able to bring BIPA claims against defendants who allegedly process their data within Illinois. The year also saw some of the most important pro-defendant developments in recent years, which collectively limit the scope of BIPA to a considerable extent. Most notably, the Ninth Circuit held that biometric data must be capable of identifying the plaintiff to be subject to BIPA, and the Illinois state legislature amended BIPA to greatly reduce the likelihood that a plaintiff may recover an astronomical damages award. In addition, district courts recognized limitations on BIPA, including that the statute doesn't apply when the defendant doesn't control the data at issue, and that a plaintiff has to plead specific facts in order to rely on a theory that her biometric data was included in an AI model's training dataset.

i. Application of BIPA to Cloud Services Companies

In a putative class action against a cloud service provider in the U.S. District Court for the Western District of Washington, a plaintiff alleged that the cloud service provider violated BIPA by allowing a third-party video game publisher to use its cloud computing services to facilitate the use of biometric data.[194] Specifically, the complaint alleged that a feature offered by the video game publisher, which allowed users to upload facial images that the game publisher then used to create a customized player resembling the user, involved the creation of a scan of face geometry (a biometric identifier under BIPA) and that the provider received the plaintiff's scan from the video game publishers, transmitted it to third-party gaming platforms, and stored it on its servers. A magistrate judge recommended that the provider's motion to dismiss be denied. The court reasoned that, despite the provider's assertion that it "had no ability to access users' biometric data and [was] unaware of [its] receipt of such information," the court must take as true the allegation that the provider "knowingly obtained" the data and that it remained in the provider's "control" as the provider "disseminate[d] and store[d] it" on its servers.[195] Thus, the court concluded that the plaintiff had plausibly alleged both the provider's "possession" and "collection" of biometric data, even absent any allegation that the provider itself had "extracted Plaintiff's face geometry."[196] The district court ultimately adopted the magistrate judge's report and recommendation,[197] and shortly thereafter, the parties reported that they had reached a settlement.[198] The outcome of this case may signal an increased risk faced by service providers based on conduct undertaken by their clients.

ii. In-State Processing of Non-Illinois Residents' Data

Customers of a sandwich chain filed a putative class action against the company, alleging that it violated BIPA by recording its drive-through customers' voice interactions and, using technology located at its corporate headquarters in Illinois, extracting from each

recording a unique voiceprint.[199] The company moved to dismiss, arguing in part that BIPA shouldn't be applied extraterritorially to two of the named plaintiffs, who visited the company's drive-throughs in Indiana and Tennessee rather than Illinois. The district court denied the motion to dismiss, reasoning that the two named plaintiffs who never used a drive-through in Illinois had nonetheless "alleged that the extraction, collection, analysis, and use of their voiceprints all occurred at Defendant's headquarters in Illinois" and that such allegations provided a sufficient nexus to Illinois.[200] However, the court was careful to qualify that "discovery may reveal that the connection to Illinois is sufficiently tenuous as to warrant revisiting the matter at the summary judgment stage."[201] The decision could lead other plaintiffs located outside the borders of the State of Illinois to bring BIPA claims under a theory that the defendant processed their biometric data within the state. It remains to be seen, however, whether other courts will be receptive to such a theory.

iii. Biometric Data Must Be "Capable of Identifying" the Plaintiff

In a notable case before the Ninth Circuit this year, a non-user of a social media platform who appeared in user-uploaded photos that the platform processed with facial-recognition technology in an effort to identify consenting users in connection with a feature that helped users tag their photos argued for a sweeping interpretation of BIPA: that the social media company needed to obtain consent to the use of facial recognition from every anonymous non-user who appeared in a photo uploaded by a user.[202] The plaintiff's reading effectively would have outlawed facial-recognition technologies like defendant's, as well as many popular biometric identification technologies, such as most biometric security systems. In the first appellate ruling of its kind, the Ninth Circuit affirmed the district court's judgment for the defendant on the ground that BIPA applies only to data that can be used to identify the plaintiff, and therefore does not apply to the anonymous data that the company created from photos of non-users for the purpose of determining whether they were users of the service who had consented to identification. The decision effectively overruled earlier rulings from courts within the Ninth Circuit, which had held that data is covered by BIPA so long as it meets the plain meaning of a "scan of face geometry"—a type of "biometric identifier" under the statute.[203] The ruling is potentially a watershed development. By its terms, the ruling significantly cabins the reach of BIPA, curtailing the ability of individuals anonymous to the defendant (such as non-users of a product or service) to bring suit under the statute. District courts have since applied this ruling to the same effect. One court in the Northern District of Illinois dismissed a BIPA claim against a consumer electronics company.[204] The plaintiff had alleged that the company collected data subject to BIPA when its technology analyzed photos on users' phones and tablets to create "unique . . . digital face templates" for each person's face, which it used to recognize the same face in multiple photos and group together photos of that same face.[205] Relying on the Ninth Circuit's ruling, the court explained that the plaintiffs failed to allege that the company had created data "capable of identifying a person's identity."[206] Although the technology "group[ed] unidentified faces together," it was the device's users who had the option to "add names to the face[]" groupings.[207] The Ninth Circuit's ruling is a significant, defense-friendly development, and its precise contours will continue to be developed through litigation at the district court level.

iv. BIPA Damages Amendment

In a sweeping decision, the Illinois Supreme Court held in 2023 that a BIPA violation accrues *each time* a private entity collects or discloses biometric data without prior

informed consent, not just upon the first collection or disclosure.[208] The court acknowledged the defendant's concerns that this broad reading of the statute could lead to "annihilative liability" but determined that "policy-based concerns about potentially excessive damage awards under [BIPA] are best addressed by the legislature."[209] The court concluded its decision with a "respectful[] suggest[ion] that the legislature review these policy concerns and make clear its intent regarding the assessment of damages under the Act."[210] In 2024, the legislature heeded the Illinois Supreme Court's call and amended BIPA to address companies' concerns about astronomical damages awards.[211] As amended, BIPA now clarifies that a plaintiff can recover from a defendant only once under section 15(b) for violations involving the collection of "the same biometric identifier or biometric information from the same person using the same method of collection" and once under Section 15(d) for violations involving the disclosure of "the same biometric identifier or biometric information from the same person to the same recipient" where such data was collected "using the same method of collection."[212] The amendment greatly reduces the likelihood that an individual plaintiff can recover an outsized damages award under the statute. However, courts are currently split on the question of whether the amendment applies retroactively.[213]

v. Defendant's Lack of Control of the Data at Issue

A plaintiff brought a putative class action against a software company under sections 15(a) and 15(b) of BIPA, alleging that the company "acquired [her facial scan] when third parties viewed her photograph with a device running the [] operating system owned and controlled by [the defendant]."[214] Notably, the plaintiff did "not allege that her biometrics were physically stored on [the defendant's] hardware."[215] The Northern District of Illinois granted the defendant's motion to dismiss. The court rejected the plaintiff's argument that the company "possess[ed]" or "collect[ed]" the alleged facial scans simply because it (1) "designed, licensed, and updated the facial scan software on users' devices"; (2) "exercised control over the device users' ability to access and use the facial scan software"; and (3) "retained the ability to control whether and how a user could use the facial scan software."[216] As the court explained, "control of the facial scan software is not the same as control of the facial scan data that is collected using the software" onto users' own devices.[217] In other words, offering "a tool that can be used to collect a facial scan is not the same as actually doing the collecting."[218] The court's decision is notable. It paves the way for defendants to seek dismissal of BIPA claims when it is clear from the face of the complaint that the alleged data at issue remains on physical devices or other hardware controlled by third parties and the defendant does not itself exercise any control over the data.

vi. Pleading Requirement for AI Model-Training Theory

A plaintiff brought suit under BIPA against the developer of a mobile app that generates avatars from photos that users upload.[219] The plaintiff had never used the defendant's app or personally uploaded his photos to it. Rather, his theory was that the defendant violated section 15(b) by training the AI model that powered the app on a publicly available dataset of five billion photos that allegedly included images of him. Without reaching the merits of the plaintiff's claims, the court dismissed the complaint for lack of standing. The court accepted the defendant's argument that the plaintiff failed to provide a sufficient basis to conclude that his photos were even included in the dataset at issue. The plaintiff simply speculated that they might be, since the dataset was purportedly assembled by scraping popular social media sites that he uses. The court's decision confirms that a

plaintiff must allege facts that make it at least plausible that his photos are at issue when predicating a lawsuit on an AI model-training theory.

vii. Other Noteworthy Developments

In a multidistrict litigation, a group of plaintiffs brought a consolidated class action complaint against a facial recognition company, alleging (among other things) that the company "covertly scraped over three billion photographs of facial images from the internet and then used artificial intelligence algorithms to scan the face geometry of each individual depicted to harvest the individuals' unique biometric identifiers and corresponding biometric information."[220] The district court denied the defendant's motion to dismiss with respect to the plaintiffs' BIPA claims, concluding that the statute applies to "biometric data extracted from photographs."[221] Then, this year, the court granted preliminary approval of a global settlement of the litigation.[222] The proposed settlement is noteworthy for its novel terms: it would provide the class members a 23% stake in the company. At then-current potential valuations, the class members' stake was estimated to be worth roughly $52 million. Counsel for the plaintiffs issued a statement that the defendant lacked the funds needed to pay a large settlement, so the parties worked instead to find "a creative solution."[223] The settlement is yet to receive final approval.

b. Texas Biometric Privacy Law Litigation

In the first-ever lawsuit filed by the Texas Attorney General under Texas's Capture or Use of Biometric Identifier Act (CUBI), Texas claimed a large social media company violated the statute by allegedly collecting biometric data without adequate consent from photos and videos that users uploaded to the platform as part of a suite of now-deprecated features relying on facial recognition technology.[224] The case had been set to go to trial in June 2024, but the parties ultimately settled, with the defendant agreeing to pay $1.4 billion without admitting liability.

c. New York Biometric Privacy Law Litigation

Beyond BIPA and CUBI, there were also noteworthy decisions involving New York City's Biometric Identifier Information Law this year.[225] A pair of decisions, one from the Southern District of New York and the other from the Western District of Washington, held that the prohibition on "profiting" from biometric data in New York City's law is limited to transactions involving the data itself and does not extend to other benefits that the defendant may derive from the use of that data. First, earlier this year, a plaintiff filed a complaint against a major live-entertainment company, alleging that the company violated New York City's law by using facial recognition software to identify and exclude from its venues attorneys employed by law firms that are involved in litigation against it.[226] The law applies where a defendant "profit[s] from the transaction of biometric identifier information," so the "question presented," the court explained, was whether the "defendant profits when it shares biometric data with a third-party vendor to facilitate" the attorneys' exclusion.[227] The court granted the defendant's motion to dismiss. It concluded that the complaint failed to allege that the defendant profited from the transaction itself, as the statute requires.[228] Rather, the complaint asserted that the defendant "profits when it *purchases* a product or service," a theory of liability that "defies common sense."[229] Second, a group of plaintiffs filed a putative class action against two

retailers, alleging that their technologies that enable customers to simply walk out of their stores with their chosen products without queuing up at the checkout line violate New York City's law.[230] The complaint alleged that one of the defendants profited from the plaintiffs' biometric data by "sharing, leasing, trading or selling its . . . devices and databases by . . . allow[ing] [the defendant] to link individuals' biometric information to other valuable forms of information[,] . . . allowing [the defendant] (or other third parties willing to pay [the defendant] for such packaged data) to make more targeted advertising, marketing, pricing, and promotional decisions."[231] The court granted the defendants' motion to dismiss. Citing the decision involving the live-entertainment company, the court rejected the plaintiffs' argument regarding the statute's profit element, concluding that "the profit Plaintiffs allege appears to 'flow from [the defendant's] employment of [a] broader program, albeit one advanced by biometric data sharing'"—an "unpersuasive" theory.[232] The court dismissed the plaintiffs' claims against the other defendant as well, reasoning that they "fail to allege sufficient facts that [the defendant] plays any part in the control of the . . . technology or otherwise share in biometric identifier information as defined" under the statute.[233]

F. Other Noteworthy Litigation

Daniel's Law Ruled Constitutional. In 2024, a federal judge rejected a constitutional challenge to Daniel's Law, a New Jersey privacy statute enacted in 2020 in response to the tragic murder of the son of a federal judge. The statute allows law enforcement officials and their immediate family members (Covered Persons) to request that any person, business, or association not disclose their home address or unpublished telephone numbers.[234] In 2023, amendments to the statute permitted Covered Persons to assign a Daniel's Law claim to a third party, and provided for actual damages (set at a minimum of $1,000 as liquidated damages) for each violation, punitive damages upon a showing of willful or reckless disregard of the law, and reasonable attorneys' fees and other litigation costs—triggering a surge of litigation against a wide range of businesses that interact with New Jersey residents.[235] In a suit involving a third-party assignee, defendants moved to dismiss the claims on the basis that Daniel's Law is unconstitutional on its face on the basis that it violated the First Amendment and that it is a strict liability statute.[236] In November 2024, the District Court of New Jersey denied the motion to dismiss and held that Daniel's Law is constitutional.[237] As a threshold matter, the court held that Daniel's Law is a privacy statute, so its content-based regulation of speech was not subject to strict scrutiny.[238] Instead, the court applied the three-factor test that the Supreme Court has used for balancing the right of privacy against the right of free speech and concluded that Daniel's Law passed this test.[239] The defendants also argued that the law was unconstitutional on its face as a strict liability statute, that it provides for actual or liquidated damages for non-compliance without regard to fault.[240] The court rejected this argument as well, concluding that "Daniel's Law must be read as imposing liability only if a defendant unreasonably disclosed or made available the home addresses and unlisted telephone numbers of covered persons after the statutory deadline had expired."[241] Due to the exposure created by the statutory penalty of actual damages or $1,000 per violation and the short response window, this ruling has significant implications for any business interacting with New Jersey residents, and businesses should implement policies and procedures for complying with take-down requests in the 10-day window. Shortly after the ruling, the court issued an order permitting the defendants to appeal,[242] so we will continue to monitor this case in 2025. ***Cellular Data as Property***. In the first appellate decision addressing whether cellular data is property, the Ninth Circuit held that cellular data can be categorized as property that is subject to conversion.[243] Plaintiffs in a class action suit sued a major technology company alleging the company performed passive data transfers using plaintiffs' cellular data without their knowledge or consent, asserting a claim for conversion under California law.[244] The court held in connection with a motion to dismiss that cellular data can constitute property for purposes of a conversion claim—which requires a showing that there is a property right at issue—because even though the data is intangible, it allows access to a cellular network, can be limited by a user's data plan, is capable of exclusive possession or control, and can be valued, bought and sold.[245] The court also held that the plaintiffs plausibly alleged the company used

their data in a way that was inconsistent with their own property interests.[246] The court observed that when the company transfers information from its own servers, the data spent during that transfer is allocated to the customer, and accordingly is treated by the wireless carrier as if it is data that the customers themselves used.[247] Therefore, the company's use of plaintiffs' cellular data to transfer the information prevented plaintiffs from using all the cellular data they purchased and was inconsistent with the plaintiffs' property interests.[248] ***Video Privacy Protection Act (VPPA) Litigation***. Courts continued to determine the scope of the VPPA in 2024. One notable case focused on a narrow liability exception under VPPA and the level of scrutiny that should apply to VPPA. The Massachusetts District Court denied a motion to dismiss a class action suit filed against a broadcasting company where plaintiffs alleged the company disclosed their PII and viewing history to third parties without their consent.[249] The company argued that their actions fell within the narrow exception for disclosures made "incident to the ordinary course of business," but the court held that the alleged "marketing, advertising, and analytics" uses of the data did not fall within the exception's permissible uses.[250] The court also held that the alleged disclosures of consumers' PII constituted commercial speech for First Amendment purposes and required application of intermediate scrutiny to VPPA, which it passed.[251] Another federal district court also dismissed a class action suit against a casino and entertainment company that owns and operates a website that offers online video games that users can access by registering for an account with their personal information.[252] The company installed a tracking tool on its website that the plaintiff alleged shares information about a users' gaming history with a third party.[253] The court held the VPPA was inapplicable because the company did not qualify as a video tape service provider under the statute.[254] The court reasoned that video games do not constitute prerecorded content that is subject to the VPPA *unless* the video game is interlaced with "cut scenes" that are similar to prerecorded video clips.[255] A California state court, meanwhile, denied class certification in a case asserting claims for invasion of privacy and for violations of the federal Wiretap Act, CIPA, and related common law claims arising from Meta's offering of "Business Tools" to HBO and its alleged tracking of users' video-viewing activities.[256] The court denied class certification because there was no classwide method to prove whether any particular video was viewed by a class member or by someone using their account: "an individualized inquiry is necessary to determine whether the data . . . reflects a particular class or subclass member's own video-viewing behavior rather than the video-viewing behavior of a friend or family member who has accessed that individual's HBO account."[257] A Georgia federal court, however, granted class certification in a VPPA case based on a similar theory as the California case above.[258] Plaintiff alleged that WebMD violated the VPPA, because by installing the "Facebook Pixel" on webmd.com, WebMD allegedly disclosed the video-viewing activity of its users to Facebook without their consent.[259] In granting Plaintiffs' motion for class certification, the court rejected WebMD's argument that an individualized inquiry would be required, noting that scenarios a user might have allowed someone else to use their computer or a video was not working at the time when the user clicked on the link were the "exceptions," not the rule.[260] Specifically, the court wrote, "WebMD does not point to any instances in which its concerns became a reality nor does it point to any evidence regarding these concerns being anything more than exceedingly rare potential exceptions . . . the idea that class certification should be denied merely due to a possibility at this stage that a website gave a 404 error or a family member used someone else's computer seems absurd."[261] ***State Video Privacy Statutes***. The Ninth Circuit upheld district court dismissals of two class action suits against two major technology companies that alleged each company violated two state privacy statutes by unlawfully retaining users' PII: The New York Video Consumer Privacy Act and the Minnesota Video Privacy Law.[262] Plaintiffs alleged that both state privacy statutes provide a private right of action for the unlawful retention of personal information, but the Ninth Circuit disagreed, holding that neither of the privacy statutes had such a private right of action.[263] **IV. CONCLUSION** In 2024, the privacy and cybersecurity landscape in the U.S. continued to be defined by an expansion of state comprehensive privacy laws, and regulatory and enforcement activity led by federal and state agencies, as well as civil litigation brought by private plaintiffs. This was driven in large part by the rapid development and advances in data-intensive technologies like generative AI, the unrelenting cyber threat posed by malicious actors and

foreign adversaries, and an increasing focus on protecting biometric data and children's online privacy. We expect these trends to continue in 2025 as existing data-intensive technologies and use cases take hold and new ones emerge. In the absence of comprehensive federal legislation, we expect federal and state agencies to continue to lead the charge on the regulatory front and continue to aggressively pursue enforcement actions against companies and individuals. However, given the shift at the federal level driven by the Trump administration's focus on deregulation, pro-innovation, and reversal of Biden-era policies around content moderation, AI, and digital assets, we expect a significant alteration in policy and enforcement priorities at the state and federal levels. We will continue to track and analyze these developments in the year ahead. [1] Del. Code, tit. 6, § 12D-103(c)(13) (Delaware Personal Data Privacy Act). [2] Iowa Code § 715D.1 to 715D.9 (Iowa Consumer Data Protection Act). [3] *See* N.J. Rev. Stat. §§ 56:8-166.1(9)(a)(9); Mont. Code § 30-14-2801 to 30-14-2817; Colo. Rev. Stat. Ann. § 6-1-1309(1). [4] "Sensitive data" is defined as "a category of personal data that includes the following:

1. Racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, except to the extent such data is used in order to avoid discrimination on the basis of a protected class that would violate a federal or state anti-discrimination law.
2. Generative or biometric data that is processed for the purpose of uniquely identifying a natural person.
3. The personal data collected from a known child.
4. Precise geolocation data." Iowa Code § 715D.1 (26).

[5] Md. Code Ann., Com. Law § 14-4605(b)(7)(iii) (Maryland Personal Information Protection Act). [6] *Id.* § 14-4607(A)(4). [7] *See* N.J. Rev. Stat. §§ 56:18-1 to 56:18-14 (New Jersey Data Privacy Act); Neb. Rev. Stat. § 87-1102(25) (Nebraska Consumer Data Privacy Act); Fla. Stat. § 501.701-22 (Florida Digital Bill of Rights); Conn. Gen. Stat. Ann. § 42-520 (Connecticut Data Privacy Act); Tex. Bus. & Com. Code §§ 541.001 to 541.205 (Texas Data Privacy and Security Act). [8] Minn. Stat. §§ 325O.01 to 325O.14 (Minnesota Consumer Data Privacy Act). [9] N.J. Rev. Stat. §§ 56:18-1 to 56:18-14 (New Jersey Data Privacy Act). [10] Tenn. Code §§ 47-18-3301 to 47-18-3315 (Tennessee Information Protection Act). [11] *Id.* § 47-18-3213(a)(1)(A). [12] Cal. Civ. Code § 1798.100 et seq. (California Consumer Privacy Act/California Privacy Rights Act); Colo. Rev. Stat. Ann. § 6-1-1308 et seq. (Colorado Privacy Act); N.J. Stat. Ann. § 56:18-1 et seq. (New Jersey Data Privacy Act). [13] *See, e.g.*, Virginia provides an opt out right of "the processing of the personal data for the purposes of . . . profiling [which is to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements automated decisionmaking] in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." Va. Code Ann. § 59.1-575, 577. [14] Conn. Gen. Stat. Ann. § 42-515; Del. Code Ann. tit. 6, § 12D-101; Fla. Stat. § 501.701; Ind. Code § 24-15-1-1; Md. Code Ann., Com. Law § 14-4601; Mont. Code Ann. § 30-14-2801; Neb. Rev. Stat. § 87-1102; N.H. Rev. Stat. Ann. § 359-T:1; R.I. Gen. Laws § 6-48.1-1; Tenn. Code Ann. § 47-18-3301; Tex. Bus. & Com. Code § 541.001. [15] Cal. Civ. Code § 1798.100; Colo. Rev. Stat. Ann. § 6-1-1308; Ky. Rev. Stat. § 367.390; Minn. Stat. § 3250.01; N.J. Stat. Ann. § 56:18-1; Or. Rev. Stat. § 646A.570; Va. Code Ann. § 59.1-575. [16] Iowa Code § 715D.1; Utah Code Ann. § 13-61-101. [17] California's law does not directly provide a right to opt out, but instructs the California Privacy Protection Agency (CPPA) to issue regulations "governing access and opt-out rights with respect to a business' use of automated decisionmaking technology." Cal. Civ. Code § 1798.185(a)(15). The CPPA has drafted regulations on automated decisionmaking that include the right to opt-out, but the regulations are not yet final. [18] Cal. Civ. Code § 1798.100; Colo. Rev. Stat. Ann. § 6-1-1308; Conn. Gen. Stat. Ann. § 42-515; Del. Code Ann. tit. 6, § 12D-101; Fla. Stat. § 501.701; Md. Code Ann., Com. Law § 14-4601; Minn. Stat. § 3250.01; Mont. Code Ann. § 30-14-2801; Neb. Rev. Stat. § 87-1102; N.H. Rev.

Stat. Ann. § 359-T:1; N.J. Stat. Ann. § 56:18-1; Or. Rev. Stat. § 646A.570; R.I. Gen. Laws § 6-48.1-1; Tex. Bus. & Com. Code § 541.001. [19] Ind. Code § 24-15-1-1; Iowa Code § 715D.1; Ky. Rev. Stat. § 367.390; Md. Code Ann.; Tenn. Code Ann. § 47-18-3301; Utah Code Ann. § 13-61-101; Va. Code Ann. § 59.1-575. [20] 16 C.F.R. § 312.5(a)(1) (2013) (requiring operators to "obtain verifiable parental consent before any collection, use, or disclosure of personal information from children"). [21] Cal. Civ. Code § 1798.100; Conn. Gen. Stat. Ann. § 42-515; Del. Code Ann. tit. 6, § 12D-101; Minn. Stat. § 3250.01; Mont. Code Ann. § 30-14-2801; N.H. Rev. Stat. Ann. § 359-T:1. [22] N.J. Stat. Ann. § 56:18-1; Or. Rev. Stat. § 646A.570. [23] Md. Code Ann., Com. Law § 14-4601. [24] Colo. Rev. Stat. Ann. § 6-1-1308; Fla. Stat. § 501.701; Ind. Code § 24-15-1-1; Iowa Code § 715D.1; Ky. Rev. Stat. § 367.390; Neb. Rev. Stat. § 87-1102; R.I. Gen. Laws § 6-48.1-1; Tenn. Code Ann. § 47-18-3301; Tex. Bus. & Com. Code § 541.001; Utah Code Ann. § 13-61-101; Va. Code Ann. § 59.1-575. [25] There is an implicit exception if businesses must retain data in order to comply with federal or state laws or regulations. Both statutes contain a blanket statement that nothing in the law should be construed to interfere with a business's ability to comply with federal or state laws or regulations. [26] As a representative example, Virginia provides that businesses may comply with a request to delete by "opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of this chapter." Va. Code Ann. § 59.1-577(b)(5). [27] States with requirement: Cal. Civ. Code § 1798.100; Colo. Rev. Stat. Ann. § 6-1-1308; Conn. Gen. Stat. Ann. § 42-515; Del. Code Ann. tit. 6, § 12D-101; Md. Code Ann., Com. Law § 14-4601; Minn. Stat. § 3250.01; Mont. Code Ann. § 30-14-2801; Neb. Rev. Stat. § 87-1102; N.H. Rev. Stat. Ann. § 359-T:1; N.J. Stat. Ann. § 56:18-1; Or. Rev. Stat. § 646A.570; Tex. Bus. & Com. Code § 541.001. [28] States with requirement: Del. Code Ann. tit. 6, § 12D-101; Minn. Stat. § 3250.01; Or. Rev. Stat. § 646A.570; R.I. Gen. Laws § 6-48.1-3(a) (requiring that "all third parties to whom the controller has sold or may sell customers' personally identifiable information" be identified in a "conspicuous location on its website"). [29] States with requirement: Del. Code Ann. tit. 6, § 12D-104(c)(5); N.J. Stat. Ann. § 56:8-166.10. [30] Fla. Stat. § 501.1736(2)(b)(1), 501.1736(3)(a). [31] *Id.* § 501.1736. [32] *Id.* [33] *Id.* § 501.1738(1). [34] *Id.* § 501.1738(2). [35] *Id.* [36] *Id.* [37] Ga. Code. Ann. § 39-6-1(3). [38] *Id.* § 39-6-2(c). [39] *Id.* § 39-6-2(a). [40] *Id.* § 39-6-1. [41] *Id.* § 39-6-2(e). [42] *Id.* § 39-6-3. [43] Md. Code Ann., Com. Law § 14-4801(e). [44] *Id.* §§ 14-4804(b); 14-4807. [45] *Id.* § 14-4801(c). [46] *Id.* § 14-4805(a). [47] Complaint, *NetChoice v. Brown*, Case No. 1:25-cv-00322-RDB (Feb. 3, 2025). [48] N.Y. General Business Law § 1500.6. [49] *Id.* § 1500.1; § 1501. [50] *Id.* § 1502. [51] Pub. Act 103-0769. [52] *Id.* [53] *Cothron v. White Castle System, Inc.*, 216 N.E.3d 918, 929 (Ill. 2023). [54] The bill defines biometric data as "one or more biometric identifiers that are used or intended to be used, singly or in combination with each other or with other personal data, for identification purposes." The bill defines "biometric identifiers" as "data generated by the technological processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual." H.B. 24-1130, 74th Gen. Assemb., Reg. Sess. (Colo. 2024). [55] Colo. Rev. Stat. Ann. § 6-1-1314(3). [56] *Id.* § 6-1-1314(2). [57] *Id.* § 6-1-1314(2)(III). [58] *Id.* § 6-1-1314(6). [59] *Id.* § 6-1-1314(4)(a). [60] *Id.* § 6-1-1314(4)(b). [61] *Id.* § 6-1-1314(5). [62] *Id.* § 6-1-1314(4)(c). [63] H.B. 24-1130, 74th Gen. Assemb., Reg. Sess. (Colo. 2024). [64] A.B. A836, 2023-2024 Leg., Reg. Sess. (N.Y. 2024); S.B. S2518-A, 2023-2024 Leg., Reg. Sess. (N.Y. 2024). [65] N.Y. Labor Law § 201. [66] *Id.* § 201-i(1)(d). [67] *Id.* § 201-i(1)(c), (6). [68] *Id.* § 201-i(2)(a). [69] *Id.* § 201-i(3)(a). [70] *Id.* § 201-i(5)(c). [71] *Id.* § 201-i(2)(b). [72] *Id.* § 201-i(5)(a)(i), (ii). [73] Cal. Health & Saf. Code § 27000.5(b)(1). [74] *Id.* § 27002(a)(1). [75] *Id.* § 27005. [76] *NetChoice, LLC v. Bonta*, No. 5:24-cv-07885-EJD (9th Cir.). [77] Colo. Rev. Stat. Ann. § 6-1-1313(16.7); Cal. Civ. Code § 1798.140(ae)(1)(G)(ii). [78] Colo. Rev. Stat. Ann. § 6-1-1313(16.7). [79] Cal. Civ. Code § 1798.140(ae)(1)(G)(ii). [80] H.B. 24-1058, 74th Gen. Assemb., Reg. Sess. (Colo. 2024); S.B. 1223, 2023-2024 Leg., Reg. Sess (Cal. 2024). [81] Colo. Rev. Stat. Ann. § 6-1-1313(2.5). [82] American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. § 2 (2024). [83] *Id.* [84] Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50(I)(2)(a). [85] Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50(I)(2)(c)(4). [86] Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50(I)(2)(c)(8). [87] H.R. 7690, 118th Cong. (2nd

Sess. 2023). [88] H.R. 7621, 118th Cong. (2nd Sess. 2023). [89] H.R. 7841, 118th Cong. (2nd Sess. 2023). [90] H.R. 8293, 118th Cong. (2nd Sess. 2023). [91] S. 4075, 118th Cong. (2nd Sess. 2023). [92] S. 4697, 118th Cong. (2nd Sess. 2023). [93] S. 3661, 118th Cong. (2nd Sess. 2023). [94] S. 5218, 118th Cong. (2nd Sess. 2023). [95] On February 20, 2025, the FTC issued a Request for Information on "how technology platforms deny or degrade … users' access to services based on the content of the users' speech or their affiliations." [96] *FTC v. NGL Labs, LLC*, No. 2:24-cv-05753-JLS-PVC (C.D. Cal. 2024). [97] *Nat'l Treasury Employees Union v. Vought*, No. 1:25-cv-381. [98] *Mayor & City Council of Baltimore v. Vought*, No. 25-cv-00458. [99] *Mayor & City Council of Baltimore v. Vought*, No. 25-cv-00458 (MJM) (Feb. 28, 2025, D. Md.). [100] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (July 26, 2023). [101] Designation of size depends on the type of Covered Institution. *See* Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer, 89 FR 47688, Table 3 (June 3, 2024) (to be codified at 17 C.F.R. pts. 240, 248, 270, 275), https://www.federalregister.gov/documents/2024/06/03/2024-11116/regulation-s-p-privacy-of-consumer-financial-information-and-safeguarding-customer-information#footnote-357-p47719. [102] Under the rule, covered persons include 1) foreign individuals who are resident in countries of concern; 2) entities that are 50% or more owned by covered persons or by countries of concern; and 3) employees or contractors of such entities or of countries of concern. [103] *See*, for example, *United States ex rel. Matthew Decker v. Pennsylvania State University*, Case No. 2:22-cv-03895-PD (E.D. Pa. Oct. 5, 2022). [104] Department of Defense, *Cybersecurity Maturity Model Certification (CMMC) Program* (2024), 32 C.F.R. § 170, https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170. [105] Consumer Guide, Federal Communications Commission, *One-to-One Consent Rule for TCPA Prior Express Written Consent Frequently Asked Questions* (Dec. 2024), DOC-408396A1.pdf (fcc.gov). [106] *Insurance Marketing Coalition, Ltd. v. Federal Communications Commission*, No. 24-10277, 2025 WL 289152 (11th Cir. Jan. 24, 2025). [107] Complaint, *Garner et al v. AT&T Inc.*, No. 3:24-cv-00962-E (N.D. Tex. 2024), ECF No. 1. [108] *Id.* [109] *Id.* [110] *Savidge v. Pharm-Save, Inc.*, 727 F. Supp. 3d 661 (W.D. Ky. 2024). [111] *Savidge v. Pharm-Save, Inc.*, 727 F. Supp. 3d 661, 675–95 (W.D. Ky. 2024). [112] *Griggs v. NHS Mgmt., LLC*, No. SC-2023-0784, 2024 WL 4797211 (Ala. Nov. 15, 2024). [113] *Id.* at *3–*8. [114] *Miller v. NextGen Healthcare, Inc.*, No. 1:23-CV-2043-TWT, 2024 WL 3543433, 1317–20 (N.D. Ga. July 25, 2024). [115] *Id.* at 1318. [116] *See, e.g.*, *D'Angelo v. FCA US, LLC*, 726 F. Supp. 3d 1179, 1187–88 (S.D. Cal. 2024). [117] *See, e.g.*, *id.* [118] *See, e.g.*, *Jackson v. LinkedIn Corp.*, 2024 WL 3823806 (N.D. Cal. Aug. 13, 2024). [119] 18 U.S.C. § 2511(2)(d). [120] 18 U.S.C. § 2520(2)(B). [121] *See* Cal. Penal Code §§ 631(a), 632(a), 637.2. [122] *See, e.g.*, *Yoon v. Meta Platforms, Inc.*, No. 24-cv-02612-NC, 2024 WL 5264041, at *4 (N.D. Cal. Dec. 30, 2024). [123] *Compare, e.g.*, *Jackson v. LinkedIn Corp.*, 744 F. Supp. 3d 986 (N.D. Cal. Aug. 13, 2024) (denying defendant's motion to dismiss California wiretapping claim), *with, e.g.*, *B.K. v. Eisenhower Med. Ctr.*, 721 F. Supp. 3d 1056, 1065 (C.D. Cal. 2024) (dismissing federal and California wiretapping claims without leave to amend). [124] *Doe I v. Google LLC*, 741 F. Supp. 3d 828, 840–41 (N.D. Cal. 2024); *see also B.K. v. Desert Care Network*, No. 2:23-cv-05021, 2024 WL 1343305, at *1, *7 (C.D. Cal. Feb. 1, 2024). [125] *See Doe I*, 741 F. Supp. 3d at 841 (noting "[i]t's possible that this ruling is contrary to Judge Orrick's analysis of intent in a similar pixel case"). [126] *See, e.g.*, *D'Angelo*, 726 F. Supp. 3d at 1193 ("The Court recognizes that there is a disagreement in this District about whether TransUnion undermined In re Facebook's holding that a violation of CIPA is sufficient to allege an injury-in-fact."). [127] *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021). [128] *Williams v. DDR Media, LLC*, No. 22-cv-03789, 2024 WL 4859078 (N.D. Cal. Nov. 20, 2024). [129] *Id.* at *1. [130] *Id.* at *2. [131] *Id.* at *5. [132] *Griffith v. TikTok, Inc.*, No. 5:23-CV-00964-SB-E, 2024 WL 5279224, at *3, *12 (C.D. Cal. Dec. 24, 2024). [133] *Id.* at *1–2. [134] *Id.* at *10. [135] *Frasco v. Flo Health, Inc.*, No. 21-cv-00757-JD, 2024 WL 4280933 (N.D. Cal. Sept. 23, 2024). [136] *Id.* at *4. [137] Unopposed Motion for Final Approval of Class Action Settlement, *Brown v. Google LLC*, No. 4:20-cv-03664-YGR-SVK (N.D. Cal. 2024), Dkt. 1098-2. [138] *Id.* at 2. [139] *Id.* [140] 18 U.S.C. § 1030(a). [141] Verdict Form, *Ryanair DAC v. Booking Holdings Inc.*, No. 1:20-cv-01191 (D. Del. 2022), Dkt. 457. [142] *Id.*, Dkt. 76. [143] *Id.* [144] *Id.*, Dkt. 457. [145] *Id.*, Dkt. 466. [146] *Id.*, Dkt. 516. [147] *Id.*, Dkt. 518. [148] *Abu v. Dickson*, 107

F.4th 508, 513 (6th Cir. 2024). [149] *Id.* [150] *Id.* at 514–15. [151] *Id.* at 515. [152] *Id.* at 516. [153] *Moonlight Mountain Recovery, Inc. v. McCoy*, No. 1:24-cv-00012-BLW, 2024 WL 4027972, at *1 (D. Idaho Sept. 3, 2024). [154] *Id.* [155] *Id.* at *4. [156] *Id.* [157] *CTI III, LLC v. Devine*, 2022 WL 1693508, at *3 (E.D. Cal. May 26, 2022). [158] Cal. Penal Code § 502(e)(1); *see also id.* § 502(c) (listing violations). [159] *Id.* § 502(b)(1). [160] *Id.* § 502(e)(1). [161] *See Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1021 (C.D. Cal. 2023) (noting that "the majority of courts to consider the issue" have found the CDAFA "contemplates some damage to the computer system, network, program, or data contained on that computer, as opposed to data generated by a plaintiff while engaging with a defendant's website"). [162] *Doe v. Cnty. of Santa Clara*, No. 23-cv-04411-WHO, 2024 WL 3346257, at *1, *11 (N.D. Cal. July 8, 2024). [163] *Id.* at *9. [164] *Esparza v. Kohl's, Inc.*, 723 F. Supp. 3d 934 (S.D. Cal. 2024). [165] *Id.*at 945 (noting "Plaintiff alleges there is a market for his data that Defendant . . . allegedly profit[s] from"). [166] *Id.* at 945. [167] 47 U.S.C. § 227. [168] *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2021). [169] *Fam. Health Physical Med., LLC v. Pulse8, LLC*, 105 F.4th 567, 575 (4th Cir. 2024). [170] *Id.* at 572–73. [171] *Id.* at 573. [172] *Career Counseling, Inc. v. AmeriFactors Fin. Grp., LLC*, 91 F.4th 202, 210 (4th Cir. 2024) [173] *Id.* [174] *McLaughlin Chiropractic Assocs., Inc. v. McKesson Corp.*, 145 S. Ct. 116 (2024). [175] Cal. Civ. Code § 1798.150(a)(1). [176] *Id.* [177] *See Johnson v. Cornerstone Nat'l Ins. Co.*, No. 22-04135, 2024 WL 5265372, at *6–7 (W.D. Mo. Apr. 29, 2024) (granting motion to dismiss where plaintiffs had alleged only that a software company had helped an insurance company design and set up a system, not that it actually accessed individuals' confidential information). [178] *In re NCB Mgmt. Serv., Inc. Data Breach Litig.*, No. 23-1236, 2024 WL 4160349, at *17–18 (E.D. Pa. Sept. 11, 2024). [179] *In re Accellion, Inc. Data Breach Litig.*, 713 F. Supp. 3d 623, 641 (N.D. Cal. 2024). [180] *Miller v. NextGen Healthcare, Inc.*, 742 F. Supp. 3d 1304, 1327 (N.D. Ga. 2024). [181] *M.G. v. Therapymatch, Inc.*, No. 23-cv-04422, 2024 WL 4219992, at *1 (N.D. Cal. Sept. 16, 2024). [182] *Id.* at *7. [183] *Id.* [184] *Owens v. Smith, Gambrell and Russell Int'l, LLP*, No. CV23-01789, 2024 WL 3914663, at *1 (C.D. Cal May 30, 2024). [185] *Id.* at *11. [186] *Id.* at *11–12. [187] *In re Eureka Casino Breach Litig.*, No. 2:23-cv-00276, 2024 WL 4253198, at *1 (D. Nev. Sept. 19, 2024). [188] *Id.* [189] *Id.* at *13. [190] *Id.* [191] *Id.* [192] *Id.* [193] *Id.* at *13–14. [194] *Mayhall v. Amazon Web Servs., Inc.*, No. C21-1473-TL-MLP, 2024 WL 3842563 (W.D. Wash. May 29, 2024). [195] *Id.* at *5. [196] *Id.* at *5–6. [197] *Mayhall v. Amazon Web Servs., Inc.*, 2:21-cv-01473 (W.D. Wash. Nov. 5, 2024), ECF No. 112. [198] *Mayhall v. Amazon Web Servs., Inc.*, 2:21-cv-01473 (W.D. Wash. Jan. 15, 2025), ECF No. 114. [199] *Polizzi v. Jimmy John's, LLC*, No. 3:23-cv-02168 (C.D. Ill. July 17, 2024), ECF No. 24. [200] *Id.* at 12. [201] *Id.* at 13. [202] *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117 (9th Cir. 2024). [203] *See, e.g.*, *Colombo v. YouTube, LLC*, 679 F. Supp. 3d 940, 944–45 (N.D. Cal. 2023). [204] *G.T. v. Samsung Elecs. Am. Inc.*, 742 F. Supp. 3d 788 (N.D. Ill. 2024). [205] *Id.* at 793 [206] *Id.* at 801. [207] *Id.* [208] *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918 (Ill. 2023), *as modified on denial of reh'g* (Ill. July 18, 2023). [209] *Id.* at 928–29. [210] *Id.* at 929. [211] 740 Ill. Comp. Stat. Ann. 14/20(b) (2024). [212] *Id.* at (b)–(c). [213] *Compare Gregg v. Central Transp. LLC.*, No. 24 C 1925, 2024 WL 4766297, at *2–3 (N.D. Ill. Nov. 13, 2024) *with Schwartz v. Supply Network, Inc.*, No. 23 CV 14319, 2024 WL 4871408 (N.D. Ill. Nov. 22, 2024). [214] *Bhavilai v. Microsoft Corp.*, 716 F. Supp. 3d 640, 641 (N.D. Ill. 2024). [215] *Id.* [216] *Id.* [217] *Id.* [218] *Id.* [219] *Brantley v. Prisma Labs, Inc.*, No. 23 C 1566, 2024 WL 3673727 (N.D. Ill. Aug. 6, 2024). [220] *In re Clearview AI, Inc., Consumer Priv. Litig.*, 585 F. Supp. 3d 1111, 1118 (N.D. Ill. 2022), *clarified on denial of reconsideration*, 2022 WL 2915627 (N.D. Ill. July 25, 2022). [221] *Id.* at 1122–23. [222] Preliminary Order of Approval of Class Action Settlement, *In re Clearview AI, Inc., Consumer Priv. Litig.*, No. 21-cv-0135 (N.D. Ill. June 21, 2024), ECF No. 580. [223] *See* Plaintiff's Unopposed Motion and Memorandum in Support of Preliminary Approval of Class Action Settlement, *In re: Clearview AI, Inc. Consumer Privacy Litigation*, 1:21-cv-00135 (N.D. Ill. June 12, 2024), ECF No. 578, at 5. [224] *State of Texas v. Meta Platforms, Inc.*, No. 22-0121 (Tex. 71st Dist. Ct., Harrison Cnty.). [225] N.Y.C. Admin. Code § 22-1202. [226] *Gross v. Madison Square Garden Ent. Corp.*, No. 23-CV-3380 (LAK) (JLC), 2024 WL 2055343 (S.D.N.Y. May 7, 2024). [227] *Id.* at *1. [228] *Id.* at *2. [229] *Id.* at *1. [230] *Mallouk v. Amazon.com, Inc.*, No. C23-852-RSM, 2024 WL 3511015, at *1 (W.D. Wash. July 23, 2024). [231] *Id.* at *5. [232] *Id.* (quoting *Madison Square Garden*, 2024 WL 2055343, at *1). [233] *Id.* at *6. [234] N.J.S.A. §

56:8-166.1. et seq. [235] *Id.* [236] *Id.* at *1. [237] *Id.* [238] *Id.* at *7–8. [239] *Id.* at *8. [240] *Id.* at *10. [241] *Id.* at *12 (predicting that the Supreme Court of New Jersey would construe Daniel's Law as requiring a covered person or assignee to establish an entity's negligence in order to obtain an award of actual or liquidated damages). [242] *See* Order, *Atlas Data Priv. Corp. v. We Inform, LLC*, No. 1:24-cv-04037 (D.N.J. Ill. Dec. 2, 2024), ECF. No. 27. [243] *Taylor v. Google, LLC*, No. 22-16654, 2024 WL 837044, at *2 (9th Cir. Feb. 28, 2024). [244] *Id.* [245] *Id.* at *1–2. [246] *Id.* at *2. [247] *Id.* [248] *Id.* [249] *Saunders et al v. Hearst Television, Inc.*, 711 F. Supp. 3d 24, 28–29 (D. Mass. Jan. 11, 2024). [250] *Id.* at 32. [251] *Id.* at 32–33. [252] *Mendoza v. Caesars Ent., Inc.*, No. 1:23-cv-03591, 2024 WL 2316544, at *1 (D.N.J. May 22, 2024). [253] *Id.* at *2. [254] *Id.* [255] *Id.* (citing *Aldana v. GameStop*, No. 22-cv-7063, 2024 WL 708589, at *6 (S.D.N.Y. Feb. 21, 2024)). [256] *McDaniel, et al. v. Meta Platforms, Inc., et al.*, Case No. 21-cv-383231 (Cal. Super. Ct. Dec. 30, 2024). [257] *Id.* [258] *Jancick v. WebMD LLC*, No. 1:22-CV-644-TWT, 2025 WL 560705 (N.D. Ga. Feb. 20, 2025) [259] *Id.* at *1. [260] *Id.* at *4. [261] *Id.* [262] *Baptiste v. Apple Inc.*, No. 23-15392, 2024 WL 1086832, at *1 (9th Cir. Mar. 13, 2024). [263] *Id.* at *2. [264] Reforming Intelligence and Securing America Act, H.R. 7888, 118th Cong. (2nd Sess. 2023). [265] *U.S. v. Hasbajrami*, No. 1:11-cr-623 (LDH), 2025 WL 258090 (E.D.N.Y. Jan. 21, 2025), superseded by *U.S. v. Hasbajrami*, No. 1:11-CR-623 (LDH), 2025 WL 447498 (E.D.N.Y. Feb. 10, 2025). [266] *See* Complaint, *De La Torre v. LinkedIn Corporation*, 5:25-cv-00709 (N.D. Cal., Jan. 21, 2025), ECF No. 1. [267] *Id.* at 5. [268] *Id.* at 14–20. [269] *See* Plaintiff's Unopposed Motion and Memorandum in Support of Preliminary Approval of Class Action Settlement, *In re: Clearview AI, Inc. Consumer Privacy Litigation*, No. 1:21-cv-00135 (N.D. Ill. June 12, 2024), ECF No. 578.

The following Gibson Dunn lawyers prepared this update: Jane Horvath, Cassandra Gaedt-Scheckter, Ashley Rogers, Natalie Hausknecht, Abbey Barrera, Jay Mitchell, Michael Brandon, Becca Smith, Jacob Arber, Trenton Van Oss, Megan Hulce, Andrew Kuntz, Viola Li, Bina Nayee, Sarah Scharf, Julie Sweeney, Nick Carey, Courtney Wang, Hayato Watanabe, Caelin Moriarity Miltko, Lauren Trujillo, Ashley Marcus, Lucy Musson, Shannon Summer, Sophia Amir, Advait Ramanan, Christina Barta, Shri Dayanandan, Sam Gensburg, Gabriela Li, Danilo Risteski, Marcus Seete, Amy Xi Shao, Ananya Subrahmanian*, and Emma Wexler.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's Privacy, Cybersecurity & Data Innovation or Artificial Intelligence practice groups: **United States**: Abbey A. Barrera – San Francisco (+1 415.393.8262, abarrera@gibsondunn.com) Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303.298.5774, rbergsieker@gibsondunn.com) Keith Enright – Palo Alto (+1 650.849.5386, kenright@gibsondunn.com) Gustav W. Eyler – Washington, D.C. (+1 202.955.8610, geyler@gibsondunn.com) Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com) Svetlana S. Gans – Washington, D.C. (+1 202.955.8657, sgans@gibsondunn.com) Lauren R. Goldman – New York (+1 212.351.2375, lgoldman@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com) Natalie J. Hausknecht – Denver (+1 303.298.5783, nhausknecht@gibsondunn.com) Jane C. Horvath – Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com) Martie Kutscher Clark – Palo Alto (+1 650.849.5348, mkutscherclark@gibsondunn.com) Kristin A. Linsley – San Francisco (+1 415.393.8395, klinsley@gibsondunn.com) Timothy W. Loose – Los Angeles (+1 213.229.7746, tloose@gibsondunn.com) Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com) Rosemarie T. Ring – San Francisco (+1 415.393.8247, rring@gibsondunn.com) Ashley Rogers – Dallas (+1 214.698.3316, arogers@gibsondunn.com) Sophie C. Rohnke – Dallas (+1 214.698.3344, srohnke@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) Frances A. Waldmann – Los Angeles (+1 213.229.7914,fwaldmann@gibsondunn.com) Debra Wong Yang – Los Angeles (+1 213.229.7472, dwongyang@gibsondunn.com) **Europe**: Ahmed Baladi – Paris (+33 1 56

43 13 00, abaladi@gibsondunn.com) Patrick Doris – London (+44 20 7071
4276, pdoris@gibsondunn.com) Kai Gesing – Munich (+49 89 189
33-180, kgesing@gibsondunn.com) Joel Harrison – London (+44 20 7071
4289, jharrison@gibsondunn.com) Lore Leitner – London (+44 20 7071
4987, lleitner@gibsondunn.com) Vera Lukic – Paris (+33 1 56 43 13
00, vlukic@gibsondunn.com) Lars Petersen – Frankfurt/Riyadh (+49 69 247 411
525, lpetersen@gibsondunn.com) Christian Riis-Madsen – Brussels (+32 2 554 72
05, criis@gibsondunn.com) Robert Spano – London/Paris (+44 20 7071
4000, rspano@gibsondunn.com) **Asia**: Connell O'Neill – Hong Kong (+852 2214
3812, coneill@gibsondunn.com) Jai S. Pathak – Singapore (+65 6507
3683, jpathak@gibsondunn.com) **Ananya Subrahmanian, an associate in New York, is not yet admitted to practice law.*

Related Capabilities

Privacy, Cybersecurity, and Data Innovation

Artificial Intelligence