GIBSON DUNN

U.S. Cybersecurity and Data Privacy Review and Outlook – 2024

Client Alert | January 29, 2024

I. Introduction In contrast to previous years, the 2023 privacy and cybersecurity landscape in the United States was not shaped by an overarching event like the COVID-19 pandemic or Russia's invasion of Ukraine. 2023 was nonetheless another groundbreaking year for privacy and cybersecurity on the regulatory and enforcement fronts. Congress's failure to pass a comprehensive privacy bill left the White House and federal agencies—along with state legislators and agencies—to lead the charge in regulating privacy and cybersecurity in the United States. The White House doubled down on its push to implement a national strategy on cybersecurity, with important implications for federal, state, and private entities. Numerous federal agencies—including the FTC, SEC, CFPB, and HHS—promulgated privacy and data protection regulations and guidance on a range of issues, including cyber-incident disclosure, children's online privacy, biometric and genetic data, artificial intelligence ("AI"), and algorithmic decision making. Many agencies also brought enforcement actions against companies and (increasingly) individuals for privacy, data security, and related violations. States were similarly active in 2023, passing and enforcing a flurry of new comprehensive state privacy laws. State agencies like the New York Department of Financial Services took aggressive steps to tighten data protection regulations for entities under their umbrella. And, while this publication does not focus on AI (a topic which will be covered in detail by Gibson Dunn's forthcoming Artificial Intelligence Legal Review), the rapid rise and proliferation of AI technology was a defining feature of the privacy and cybersecurity landscape in 2023. Litigation likewise remained active, with notable upticks in claims by private litigants and government entities related to data breaches, federal and state wiretapping laws, and state biometrics laws. We expect these trends to accelerate in 2024 and beyond, as the body of privacy and cybersecurity regulation matures and expands. This Review contextualizes these and other 2023 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, digital, telecommunications, wiretapping, and biometric information privacy laws; 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 and Review. **Table of Contents**

Related People

Cassandra L. Gaedt-Sheckter

Natalie J. Hausknecht

Martie Kutscher Clark

Timothy W. Loose

Abbey A. Barrera

Jacob U. Arber

Tony Bedel

Matt Buongiorno

Wesley Sze

Terry Wong

Michael Brandon

Lane Corrigan

Justine Deitz

Skylar Drefcinski

Erin Kim

Brendan Krimsky

Ruby B. Lang

Ignacio Martinez Castellanos

Mason W. Pazhwak

John Ryan

Becca Smith

Graham M. Stinnett

Cydney L. Swain

Julie Sweeney

Trenton J. Van Oss

Hayato Watanabe

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

II. Regulation of Privacy and Data Security Since 2018, 14 states have enacted comprehensive data privacy legislation. Five of these are currently effective, and the remaining nine will go into effect between 2024 and 2026. A number of additional state legislatures considered comprehensive consumer privacy laws this past year but have yet to enact them. In addition, several states have passed narrower data privacy laws governing the use of specific categories of information, such as health and genetic information. These laws demonstrate the states' efforts to ensure the protection of consumers' data in the absence of a comprehensive federal data privacy law. We highlight several of these state privacy laws below and provide an overview of key similarities and differences. **A. Regulation of Privacy and Data Security 1. State Legislation and Related Regulations a. Comprehensive State Privacy Laws** California was the first state to adopt a comprehensive data privacy law with the enactment of the California Consumer Privacy Act ("CCPA") in 2018. The California Privacy Rights Act ("CPRA") amended the CCPA in 2020. Since then, 13 other states—Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia—have followed California in enacting comprehensive privacy laws. As shown in the below list of comprehensive state privacy laws enacted to date, five went into effect in 2023, an additional four will go into effect in 2024, four in 2025, and one in 2026. Most of these generally align with the standard template created by the comprehensive state privacy laws in Virginia, Colorado, Connecticut, and Utah, with a few having unique features, which are highlighted below. Please see last year's Review for a more detailed assessment of the comprehensive data privacy laws in California, Virginia, Colorado, Connecticut, and Utah, which have all now gone into effect. *Table 1: Comprehensive State Privacy Laws*

Law		Enacted Date
California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights		CCPA: June 28, 2018 CPRA: November 3, 2020

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Act (CPRA)[1]	
Virginia Consumer Data Protection Act (VCDPA)[2]	March 2, 2021
Colorado Privacy Act (CPA)[3]	July 7, 2021
Connecticut Data Privacy Act (CTDPA)[4]	May 10, 2022
Utah Consumer Privacy Act (UCPA)[5]	March 24, 2022
Florida Digital Bill of Rights (FDBR)[6]	June 6, 2023
Texas Data Privacy and Security Act (TDPSA)[7]	June 18, 2023
Oregon Consumer Privacy Act (OCPA)[8]	July 18, 2023
Montana Consumer Data Privacy Act (MTCDPA)[9]	May 19, 2023
Iowa Consumer Data Protection Act (ICDPA)[10]	March 29, 2023
Delaware Personal Data Privacy Act (DPDPA)[11]	September 11, 2023
New Jersey Data Privacy Act (NJDPA)[12]	January 16, 2024
Tennessee Information Protection Act (TIPA)[13]	May 11, 2023
Indiana Consumer Data Protection Act (INCDPA)[14]	May 1, 2023

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

The tables below review core aspects of these laws, including applicability, exemptions, data subject rights, data controller obligations, and enforcement. **i. Applicability** Each comprehensive state privacy law applies to entities that conduct business in that state or provide products and services to residents of that state, and that meet certain applicability thresholds. As shown in Table 2 below, these thresholds typically relate to a company's annual gross revenue and/or the number of individuals whose personal information the business processes or controls. California is unique in applying its comprehensive privacy law to companies that derive 50% or more of their revenue from selling California residents' personal information, without pairing that requirement with a minimum number of consumers whose data is processed. Florida and Texas also have distinct requirements: Florida's statutory thresholds are designed to limit the application of the law to large companies, and Texas's law does not carry any fixed numerical thresholds with respect to gross revenue or number of consumers' whose data is processed. Unless otherwise indicated, all thresholds listed below are disjunctive requirements. *Table 2: Applicability of Comprehensive State Privacy Laws*

Law	Annual Gross Revenue	Annual Processing of Consumers' Data	Other T
CCPA/CPRA (California)	$25 million or more.	Buys, sells, or shares the personal information of 100,000 or more California residents, households, or devices.	Derives 50% or revenue from residents' per
VCDPA (Virginia)	N/A	Controls or processes the personal data of at least 100,000 Virginia consumers.	Controls or proc data of at least and derives c revenue from t
CPA (Colorado)	N/A	Processes the personal data of more than 100,000 Colorado individuals.	Derives reve discounts on g exchange for t data of 25,000
CTDPA (Connecticut)	N/A	Controls or processes the personal data of at least 100,000 Connecticut consumers.	Controls or proc data of at least and derives c revenue from t info
UCPA (Utah)	$25 million or more.	Controls or processes the personal data of 100,000 or more Utah consumers.	Controls or proc data of 25,0 consumers and of gross annual

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

			perso
FDBR (Florida)	$1 billion or more.	N/A	(i) Derives 50% annual reven advertising or th (ii) operates a speaker and voi with an integrat through a cloud free verbal activa an app store t 250,000 softwa consumer
TDPSA (Texas)	N/A	N/A	(i) Conducts bu produces produc consumed by re processes or en personal data qualify as a smal by the United St Administrat exce
OCPA (Oregon)	N/A	Controls or processes the personal data of 100,000 or more Oregon consumers, other than for completing a payment transaction.	Controls or proc data of 25,00 consumers and of gross reve perso
MTCDPA (Montana)	N/A	Controls or processes the personal data of 50,000 or more Montana consumers, excluding for the purpose of completing payment transactions.	Controls or proc data of 25,000 consumers and 25% of gross re perso
ICDPA (Iowa)	N/A	Controls or processes the personal data of 100,000 or more Iowa consumers.	Controls or proc data of 25,0 consumers and

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

			50% of gross re of pers
DPDPA (Delaware)	N/A	Controls or processes the personal data of at least 35,000 Delaware residents, excluding for the purpose of completing payment transactions.	Controls or proc data of at leas residents and de of its gross reve perso
NJDPA (New Jersey)	N/A	Controls or processes the personal data of at least 100,000 New Jersey consumers.	Controls or proc least 25,000 Ne and derives rev financial benefit
TIPA (Tennessee)	$25 million or more.	Controls or processes the personal data of 170,000 or more Tennessee consumers.	Controls or proc data of 25,000 consumers and 50% of gross re personal
INCDPA (Indiana)	N/A	Controls or processes the personal data of 100,000 or more Indiana residents.	Controls or proc data of 25,00 consumers wh derives more revenue from t

ii. Exemptions All comprehensive state privacy laws also have exemptions for certain entities and categories of data. For example, non-profit entities and entities subject to the GLBA are exempt under most comprehensive state privacy laws. HIPAA-regulated data (but not necessarily entities regulated by HIPAA generally), employee data, and business contact data are likewise typically exempt under all comprehensive state privacy laws, except for in California. California is the only state whose GLBA exemption applies only at the data level, but not the entity level. Other exemptions not included below might include entities or data regulated by other laws, such as the Fair Credit Reporting Act, Driver's Privacy Protection Act, Children's Online Privacy Protection Act, the Family Educational Rights and Privacy Act, the Farm Credit Act, and the Airline Deregulation Act. Table 3 below provides a non-exhaustive list of common exemptions. *Table 3: Exemptions in Comprehensive State Privacy Laws*

Law	Non-Profits (generally)	Consumers Engaged in a Commercial or Employment	HIPA the d le

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

			Context (i.e., employees and business contacts)	
CCPA/CPRA (California)	N		N	
VCDPA (Virginia)	N		Y	
CPA (Colorado)	Y		Y	
CTDPA (Connecticut)	N		Y	
UCPA (Utah)	N		Y	
FDBR (Florida)	N		Y	
TDPSA (Texas)	N		Y	
OCPA (Oregon)	Y		Y	
MTCDPA (Montana)	N		Y	
ICDPA (Iowa)	N		Y	
DPDPA (Delaware)	Y		Y	
NJDPA (New Jersey)	N		Y	
TIPA (Tennessee)	N		Y	
INCDPA (Indiana)	N		Y	

iii. Data Subject Rights All comprehensive state privacy laws that have been enacted or are in effect provide consumers with the right to access their data, data portability, opt-out of the sale of their data and use of certain data in connection with targeted advertising, and the right to not be discriminated against for exercising their rights. They also provide covered entities with the ability to verify or authenticate the identity of a consumer looking to exercise her rights. However, there are additional rights that are provided by some, but not all, comprehensive state privacy laws. These are outlined in Table 4 below. *Table 4: Data Subject Rights in Comprehensive State Privacy Laws*

Law	Correct Inaccurate Data	Request a List of Third Parties with Whom Data Has	Opt-Out of the Use of Data for Certain Profiling	Limit the Use and Disclosure of Sensitive Data	Appeal the Denial of Data Subject Rights Requests	

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

		Been Disclosed				R
CCPA/CPRA (California)	Y	N	Y	Limit use	N	
VCDPA (Virginia)	Y	N	Y	Opt-in	Y	
CPA (Colorado)	Y	N	Y	Opt-in	Y	
CTDPA (Connecticut)	Y	N	Y	Opt-in	Y	
UCPA (Utah)	N	N	N	Opt-out	N	
FDBR (Florida)	Y	N	Y	Opt-in	Y	
TDPSA (Texas)	Y	N	Y	Opt-in	Y	
OCPA (Oregon)	Y	Y	Y	Opt-in	Y	
MTCDPA (Montana)	Y	N	Y	Opt-in	Y	
ICDPA (Iowa)	N	N	N	Opt-out	Y	
DPDPA (Delaware)	Y	N	Y	Opt-in	Y	
NJDPA (New Jersey)	Y	N	Y	Opt-in[15]	Y	
TIPA (Tennessee)	Y	N	Y	Opt-in	Y	

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

INCDPA (Indiana)	Y	N		Y	Opt-in	Y

iv. Data Controller Obligations All comprehensive state privacy laws impose certain obligations on data controllers (entities that determine the purposes and means of processing of personal data). These include: data minimization; purpose limitations; maintaining privacy policies; maintaining reasonable administrative, technical, and physical data security controls; and contractually obligating personal data processors or service providers to comply with the applicable law. Data minimization in particular may be a significant requirement, as it requires companies to only keep data as long as they have a business need and promptly delete it thereafter. Some of the privacy laws impose additional obligations, which are outlined in Table 5 below. Specifically, some laws require (a) data protection impact assessments, which are designed to identify and minimize data protection risks, (b) financial incentive notices, which disclose discounts or other incentives that are provided in exchange for providing personal information, and (c) specific contractual requirements that set forth how vendors that process data on a business's behalf will act. *Table 5: Data Controller Obligations in Comprehensive State Privacy Laws*

Law	Data Prot Ass
CCPA/CPRA (California)	Y (no
VCDPA (Virginia)	
CPA (Colorado)	
CTDPA (Connecticut)	
UCPA (Utah)	
FDBR (Florida)	
TDPSA (Texas)	
OCPA (Oregon)	
MTCDPA (Montana)	
ICDPA (Iowa)	
DPDPA (Delaware)	
NJDPA (New Jersey)	
TIPA (Tennessee)	
INCDPA (Indiana)	

v. Enforcement Finally, there are differences between how each of these comprehensive state privacy laws are enforced and the penalties for noncompliance. As a general matter, comprehensive state privacy laws provide state attorneys general with sole enforcement authority. To date, the state laws have notably not provided for a private right of action. The only outlier is the CCPA/CPRA, which provides a limited private right of action for consumers affected by data breaches, under certain circumstances. Many states also provide for a right to cure, meaning that a plaintiff must provide a putative defendant with notice and an opportunity to cure the violation prior to bringing suit. The enforcement

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

mechanisms provided for by each comprehensive state privacy law are outlined in Table 6 below. *Table 6: Enforcement of Comprehensive State Privacy Laws*

Law		Private Right of Action	Enforcement Au
CCPA/CPRA (California)		Y[16]	California Atto General and Ca Privacy Prote Agency
VCDPA (Virginia)		N	Virginia Attor General
CPA (Colorado)		N	Colorado Atto General and district attorn
CTDPA (Connecticut)		N	Connecticut At General
UCPA (Utah)		N	Utah Attorney G and Utah Divis Consumer Prot
FDBR (Florida)		N	Florida Departm Legal Affai

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

TDPSA (Texas)		N	Texas Attorney
OCPA (Oregon)		N	Oregon Atto General
MTCDPA (Montana)		N	Montana Atto General
ICDPA (Iowa)		N	Iowa Attorney G
DPDPA (Delaware)		N	Delaware Depar Justice
NJDPA (New Jersey)		N	New Jersey At General
TIPA (Tennessee)		N	Tennessee Att General
INCDPA (Indiana)		N	Indiana Atto General

b. Other State Privacy Laws In addition to the comprehensive state privacy laws discussed above, states have continued to legislate in narrower areas, particularly with relation to health or genetic information. **i. Washington's My Health My Data Act** On April 27, 2023, Washington Governor Jay Inslee signed the "My Health My Data Act" ("MHMDA") into law, modifying the legal landscape with respect to health-related data for certain Washington entities.[17] The MHMDA creates a privacy regime focused on personal health data. ***Covered Entities.*** The MHMDA applies to "regulated entities" that process "consumer health data." The law defines "regulated entity" as any "legal entity" that: (1) "[c]onducts business in Washington or produces or provides products or services that are targeted to consumers in Washington"; and (2) "determines the purpose and means of collecting, processing, sharing, or selling of consumer health data," whether "alone or jointly with others."[18] Practically, the law applies to any entity that does business in Washington and collects or processes consumer health data. Government agencies, tribal nations, and service providers that are contracted to process consumer health data on behalf of a government agency are exempt from this definition and not considered regulated entities.[19] "Small businesses" are not exempt from the MHMDA, but are given an extra three months to comply.[20] ***Covered Data.*** The law defines "consumer health data" as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."[21] Examples of this type of data include surgeries or other health-related procedures, reproductive or sexual health information, and genetic data.[22] The primary statutory

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

carveout from the definition of “consumer health data” is information “used to engage in public or peer-reviewed scientific, historical, or statistical research.”[23] However, the research must be monitored by an independent oversight entity that implements safeguards to mitigate privacy risks, including the risk associated with the reidentification of consumer data.[24] The Washington Attorney General, who is charged with enforcing the MHMDA, has explained that purchases of “toiletry products (such as deodorant, mouthwash, and toilet paper)” do not qualify as “consumer health data,” even though they relate to “bodily functions,” whereas “an app that tracks someone’s digestion or perspiration is collecting consumer health data.”[25] ***Key Requirements.*** The MHMDA prohibits regulated entities from collecting or sharing consumer health data without first satisfying certain notice and consent requirements, including: requiring regulated entities to maintain a “consumer health data privacy policy” linked to on their homepage that discloses:

- the categories of consumer health data collected and the purpose for which the data is collected;
- the categories of sources from which the consumer health data is collected;
- the categories of consumer health data shared; and
- a list of the categories of third parties and specific affiliates with whom the regulated entity shares the consumer health data.[26]

Regulated entities may only collect or share consumer health data if a consumer provides a prior “clear affirmative act” expressing consent, or if the collection is “necessary to provide a product or service that the consumer . . . has requested.”[27] ***Consumer Rights.*** The MHMDA also provides consumers with a number of protections, including the right to: (1) confirm whether a regulated entity is collecting, sharing, or selling their consumer health data; (2) access that data; (3) withdraw consent for the collection and sharing of their consumer health data; and (4) delete their data.[28] ***Enforcement.*** A violation of the MHMDA is considered a violation of the Washington Consumer Protection Act.[29] The Washington Attorney General may enforce the law.[30] Consumers may also pursue private actions for violations of the MHMDA.[31] **ii. Montana’s Genetic Information Privacy Act** On June 7, 2023, Montana Governor Greg Gianforte signed into law the “Montana Genetic Information Privacy Act” (“MTGIPA”). The MTGIPA applies to any entity that offers consumer genetic testing products or services directly to a consumer, or collects, uses, or analyzes genetic data.[32] “Genetic data” is defined as “any data, regardless of format, concerning a consumer’s genetic characteristics.”[33] The MTGIPA requires covered entities to provide a privacy policy and notice regarding their use of genetic data and to obtain a consumer’s “express consent” in order to collect, use, or disclose a consumer’s genetic data.[34] The MTGIPA also requires an entity to “develop, implement, and maintain a comprehensive security program to protect a consumer’s genetic data against unauthorized access, use, or disclosure.”[35] The Montana Attorney General has sole authority to enforce the MTGIPA.[36] **iii. California’s Delete Act** On October 10, 2023, California Governor Gavin Newson signed the “Delete Act” into law.[37] The law revises California’s data broker registration law and gives consumers the right to manage data held by data brokers free of charge by submitting a single deletion request to a centralized website.[38] After a deletion request is submitted, a data broker is required to delete data within 45 days, and continue deleting any personal information collected about that consumer at least every 45 days thereafter.[39] After a consumer has submitted a deletion request, data brokers are also prohibited from selling or sharing new personal information about the consumer in the future.[40] Consumers will have the option to “selectively exclude” data brokers when submitting a deletion request.[41] The law also requires data brokers to “undergo an audit by an independent third party to determine compliance” with the law.[42] Under the law, a “data broker” is defined as “a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.”[43] But the law includes exemptions for entities covered by the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Insurance Information and Privacy Protection Act, the Confidentiality of Medical

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Information Act, or HIPAA, and business associates of covered entities under the Confidentiality of Medical Information Act or HIPAA.[44] **iv. New York Department of Financial Services' Amendments to Part 500 Cybersecurity Rules** On November 1, 2023, the New York State Department of Financial Services ("NYDFS") issued its Second Amendment to 23 NYCRR Part 500 ("Part 500"), which establishes numerous cybersecurity requirements for regulated entities.[45] As discussed in more depth in our recent client alert, the amendments to Part 500 include: expanded responsibility for senior governing bodies, obligations to implement additional safeguards, new requirements for larger companies, new and increased obligations related to written policies and procedures, heightened requirements around audits and risk assessments, and additional reporting requirements for cybersecurity incidents. NYDFS is responsible for enforcing Part 500 and has brought several enforcement actions against various financial entities, including banks, money transfer service providers, and cryptocurrency service providers.[46] **v. New Child Social Media Laws** Several states passed laws restricting social media apps, but those laws have been challenged in the courts. For example, Utah's Social Media Regulation Act[47] requires social media companies with at least 5,000,000 account holders worldwide to verify the age of adults seeking to maintain or open social media accounts; obtain parental consent for users under the age of 18 to open an account; imposes restrictions on children's accounts; and prohibits collections of certain data and targeted advertising.[48] The law may be enforced by either the Division of Consumer Protection or through a private right of action.[49] Plaintiffs may obtain up to $2,500 in statutory damages per violation, in addition to attorney's fees and costs.[50] The law has been challenged in two different suits that are ongoing.[51] A similar law in Arkansas that would require parental permission for children to create certain social media accounts was blocked by a federal judge.[52] The judge concluded in granting the preliminary injunction that the law, as written, was unconstitutionally vague because it failed to adequately define "social media company," and therefore which entities were subject to its requirements.[53] The judge also agreed that the law likely violates the First Amendment because the age verification process would chill speech by deterring adults from signing up for social media accounts and that the law is unnecessarily overbroad insofar as it attempts to protect minors from harmful or obscene content.[54] And a Montana federal judge blocked a law in that state that would prohibit mobile application stores from offering TikTok to Montana users.[55] The court, in granting the preliminary injunction, found that plaintiffs were likely to succeed on the merits of their arguments—namely, that an outright ban on a specific app likely violates the First Amendment, the Commerce Clause, and is preempted by federal national security law, among other reasons.[56] **2. Federal Legislation a. Comprehensive Federal Privacy Legislation** Comprehensive federal privacy legislation remains a popular, yet unrealized, objective despite recent congressional efforts. The American Data Privacy and Protection Act ("ADPPA") introduced in 2022 was the most advanced attempt to-date at enacting a comprehensive federal privacy bill. However, the bill died when it failed to advance to the House or Senate floors before the last Congress adjourned in January 2023.[57] As proposed, the ADPPA bill required covered companies to engage in "data minimization" and adopt "privacy by design" principles.[58] The ADPPA also prohibited covered entities from designing and employing discriminatory algorithms, and required them to study the impacts of their algorithms.[59] Government enforcement of the ADPPA would have been left largely to the FTC at the federal level, alongside state attorneys general and other key state officials.[60] But the ADPPA's addition of a private right of action was a source for serious concern due to the burden and cost of class action lawsuits.[61] The bill also explicitly preempted most state privacy laws—a fact that some believe was largely responsible for the bill's demise.[62] Calls for comprehensive federal privacy legislation continued throughout 2023 despite the ADPPA's failure. In the spring, Congress held hearings on the continuing need for such legislation.[63] President Biden echoed these calls in an executive order (which also enacted AI safety measures).[64] In his 2023 State of the Union address, the President likewise called for stronger online privacy protections for children.[65] **b. Other Introduced Legislation** Congress did not pass any privacy laws in 2023, although a significant number of consumer and individual privacy-related legislation was introduced.[66] This proposed privacy legislation covered a range of topics, including surveillance technologies, health privacy, privacy for children online, facial

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

recognition, AI, and cybersecurity. Many of the measures 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). Nevertheless, in the absence of comprehensive federal privacy legislation, Congress may still be more likely to enact legislation on a narrower topic that draws more bipartisan support, such as children's online safety, in the future.[67] Lawmakers focused in particular on digital privacy and safety in 2023, especially for children on social media. They held widely publicized hearings on the topic, bringing in social media executives for questioning, with more hearings to come in 2024.[68] In July 2023, the U.S. Senate Commerce Committee advanced a pair of measures seeking to put more responsibility on social media platforms to ensure child safety online: the Kids Online Safety Act, which would require platforms to enact measures to prevent harms to minors and to restrict targeted advertising for children under 13;[69] and COPPA 2.0, which would upgrade and expand the original children's online privacy law, including by adding protections for teens ages 13 to 16.[70] Other privacy bills introduced in 2023 include: the Informing Consumers about Smart Devices Act (requiring manufacturers to disclose that a camera or microphone is part of a device before purchase),[71] the Stop Spying Bosses Act (requiring disclosure of or prohibiting surveillance, monitoring, and collection of worker data),[72] the UPHOLD Privacy Act (establishing protection for personally identifiable health and location data),[73] the DELETE Act (requiring the FTC to establish a system allowing individuals to request that data brokers delete their personal information),[74] the Data Care Act of 2023 (imposing duty of care, loyalty, and confidentiality on online service providers),[75] the Online Privacy Act of 2023 (establishing individual privacy rights and creating a private right of action and Digital Privacy Agency),[76] and others described in this Review. Congress also considered cybersecurity-related legislation: the Federal Cybersecurity Vulnerability Reduction Act of 2023 (requiring certain government contractors to adopt vulnerability disclosure policies),[77] the Modernizing the Acquisition of Cybersecurity Experts Act of 2023 (generally barring agencies from setting minimum educational requirements for cybersecurity workers),[78] and the Federal Cybersecurity Workforce Expansion Act (providing training and apprenticeships for cybersecurity workers).[79] **B. Enforcement and Guidance** In 2023, government regulators remained active in enforcement and regulatory efforts related to data privacy, cybersecurity, and new technology. This section summarizes notable regulatory and enforcement efforts by the Federal Trade Commission ("FTC"), Consumer Financial Protection Bureau ("CFBP"), Securities and Exchange Commission ("SEC"), Department of Health and Human Services ("HHS"), and other federal and state agencies. **1. Federal Trade Commission** The FTC remained active in the regulation and enforcement of cybersecurity and data privacy in 2023—and continued to aggressively pursue new regulatory, enforcement, and litigation matters in other areas as well. Several actions, such as its rulemaking on junk fees, have had important impacts on online businesses. For example, the proposed junk fees rule was introduced in direct response to President Biden's announced priorities for consumer protection' and following his call for transparency in consumer pricing.[80] The FTC extended the comment period for the rule through February 7, 2024.[81] As currently drafted, the rule would ban "hidden fees"—or fees that are mandatory, even if provided by a different entity. It would also ban "misleading fees," essentially requiring disclosure of the purpose and refundability of any fees charged. The FTC also continued to prioritize 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 on these topics in 2023. **a. FTC Organization Updates** In March 2023, Republican Commissioner Christine Wilson resigned abruptly from the FTC, publicly citing her disagreements with Chair Lina Khan's vision and management of the FTC.[82] This created an additional vacancy on the five-member commission, following the departure of Commissioner Noah Phillips in October 2022. In July 2023, President Joe Biden nominated two Republican replacements: Virginia Solicitor General Andrew Ferguson and Utah Solicitor General Melissa Holyoak.[83] Prior to his current appointment as Virginia Solicitor General, Ferguson served in numerous roles on the Hill, including as Chief Counsel to Senate Minority Leader Mitch McConnell, as Chief

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Counsel for Nominations and the Constitution to then-Judiciary Committee Chairman Lindsey Graham, and as Senior Special Counsel to then-Judiciary Committee Chairman Chuck Grassley. Holyoak previously served as President and General Counsel of a nonprofit public-interest law firm that advocates for free markets, free speech, and limited government. In their confirmation hearing, both Holyoak and Ferguson demonstrated interest in regulating big technology companies. Holyoak specifically called out the importance of protecting children online.[84] Both nominations are currently held up in the Senate.[85] If confirmed, the new Commissioners will not change the Republican-Democrat balance of power at the FTC, which has been led by a Democratic majority since Commissioner Bedoya was confirmed in 2022. **b. Algorithmic Bias and Artificial Intelligence** The FTC continues to signal that AI and algorithms are an enforcement priority. In a mid-year public editorial, for instance, FTC Chair Lina Kahn warned of the risks AI poses, including producing discriminatory outcomes and potential privacy violations.[86] As reflected in Chair Khan's editorial, the FTC is particularly concerned about the effects algorithms may have on consumer privacy, including the use of consumer data to train large language models and inadvertent disclosure of personally identifiable information ("PII") through chatbots. In a series of AI-focused blog posts published from February to August 2023, the FTC warned businesses that they should avoid using automated tools that result in biased or discriminatory impacts. One post further noted that businesses "can't just blame a third-party developer of the technology" when reasonably foreseeable failures occur; instead, businesses should investigate and identify the foreseeable risks and impact of AI before using it in a consumer-facing setting.[87] In March 2023, the FTC also specifically called out AI technology that simulates human activity and can be used by third-party bad actors to, among other things, target communities of color with fraudulent schemes."[88] It warned that businesses considering launching tools with such risks must employ deterrents that go beyond "bug corrections or optional features that third parties can undermine via modification or removal."[89] Other use cases highlighted by the FTC as targets for enforcement include: technology that enables "deepfakes" and "voice cloning,"[90] customizing ads to specific people or groups in a manner that "trick[s] people into making harmful choices[,]"[91] and tools that purport to detect generative AI content.[92] For a more detailed discussion of regulatory developments in AI, please see Gibson Dunn's forthcoming Artificial Intelligence Legal Review. **c. Commercial Surveillance and Data Security i. FTC's Approach to Data Security** In a February 2023 blog post, the FTC's Deputy Chief Technology Officer Alex Gaynor highlighted three best practices for effectively protecting user data drawn from recent FTC orders: (i) requiring multi-factor authentication (for consumers and employees); (ii) requiring a company's systems connections to be encrypted and authenticated; and (iii) requiring data retention schedules to be published and followed.[93] Gaynor warns that these practices alone "are not the sum-total of everything the FTC expects from an effective security program."[94] He nevertheless suggests a security program is highly likely to be effective if it incorporates these practices.[95] **ii. Rulemaking on Commercial Surveillance and Data Security** As described in Gibson Dunn's prior alert, the FTC's Advance Notice of Proposed Rulemaking on commercial surveillance and data security would overhaul the regulatory landscape for corporate internet use. FTC Consumer Protection Chief Samuel Levine noted in a speech in September 2023 that the FTC is currently reviewing over 11,000 comments received in response to the request for comment, which closed on November 21, 2022.[96] If adopted, the rule will have widespread impact, implicating every facet of the internet from advertising to algorithmic decision-making. The advanced notice for the proposed rule, for instance, seeks comment on issues as wide ranging as whether consumer consent is still an effective gatekeeper for corporate data practices, whether the FTC should forbid or limit the development, design, and use of certain automated decision-making systems, and whether the FTC should adopt workplace, teen, or industry-specific (e.g., health- or finance-related) rules around data collection and use. The FTC is expected to take final action on the proposed rule in 2024.[97] **d. Notable FTC Enforcement Actions** In 2023, the FTC maintained its aggressive stance on privacy enforcement, which has been a hallmark of Chair Khan's tenure. In addition to enforcement actions that hold companies responsible for the activities discussed, there has also been a rise in actions brought against individuals. Below we discuss some of the

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

FTC's most notable enforcement actions in 2023. ***Video Game and Software Developer.*** In March 2023, the FTC finalized an order in an action originally described in last year's Review, which will require a large video game and software developer to pay $245 million to refund affected consumers and bans the company from charging consumers through the use of "dark patterns" or otherwise charging consumers without obtaining their affirmative consent.[98] The order also bars the company from blocking consumers' access to their accounts if the consumer is disputing unauthorized charges. ***Home Security Camera Company.*** The FTC brought an action under Section 5(a) of the FTC Act,[99] challenging a security camera company's representations regarding security, and alleging that employees and contractors were able to access private videos.[100] A proposed settlement would require deletion of certain data and affected data products "such as data, models, and algorithms derived from videos it unlawfully reviewed," establishment of a privacy and data security program, obtaining assessments by a third party, and cooperation with a third-party assessor.[101] ***Tax Preparation Firms.*** The FTC issued Notices of Penalty Offenses to five tax preparation firms about the use of information collected for tax preparation services to solicit loan borrowers. A Notice of Penalty Offense is intended to put companies on notice of prior successful enforcement actions against other companies, but does not mean the FTC has found the recipients are violating the law.[102] However, the FTC's Notice warned that the companies could face civil penalties of up to $50,120 per violation if they use or disclose consumer confidential data collected for tax preparation for other purportedly unrelated purposes, such as advertising, without express consumer consent.[103]
Voice Assistant. In May, DOJ brought an action on behalf of the FTC against a major technology company that includes, among its products, a voice assistant.[104] The FTC alleged that the company improperly prevented parents from deleting their children's data and retained and risked exposure of sensitive data. The FTC's settlement with the company, approved in July 2023, requires the company to overhaul its deletion practices, as well as implement stronger privacy safeguards to settle Children's Online Privacy Protection Act Rule ("COPPA Rule") claims and deception claims about its data deletion practices.[105] ***Telehealth and Prescription Drug Provider.*** The FTC brought its first enforcement action under the Health Breach Notification Rule, which was originally adopted in 2009 and requires vendors of personal health records and related entities to notify consumers, the FTC, and, in some cases, the media, when such data is disclosed or acquired without consumers' authorization.[106] The FTC alleged that the company failed to notify consumers, the FTC, and the media about its disclosure of individually identifiable health information to certain online services. This enforcement action followed a 2021 FTC policy statement that purported to require health apps and other online services to comply with the Health Breach Notification Rule.[107] The company agreed to pay a $1.5 million civil penalty and is barred from sharing user health data with third parties for advertising.[108] The FTC also proposed amendments to the Health Breach Notification Rule, with a public comment period that ended on August 8, 2023.[109] ***Genetic Testing Firm.*** The FTC settled allegations against a genetic testing firm for allegedly leaving user data unprotected, misleading users about their ability to delete their data, and retroactively changing its privacy policy without proper notice to consumers. In addition to monetary penalties of $75,000, as part of the final order, the company is required to take remedial actions including instructing third-party contractors to destroy all DNA samples retained beyond a specified timeframe, notifying the FTC of any unauthorized disclosure of consumer personal health data, and implementing a comprehensive information security program.[110] ***In-Store Surveillance and Facial Recognition.*** For the first time, the FTC alleged that the use of facial recognition technology may be an unfair practice or deceptive under Section 5 of the FTC Act.[111] The FTC alleged that a national pharmacy chain deployed AI-facial recognition technology to identify shoplifters and other problematic shoppers. The FTC's complaint alleged that the company failed to take reasonable measures to prevent harm to consumers who were erroneously accused by employees of wrongdoing because the technology incorrectly flagged the consumers as matching the profile of a known shoplifter or troublemaker. The FTC banned the retailer's use of facial recognition technology for five years. While the FTC also alleged the company violated the terms of a 2010 consent decree by failing to comply with its own information security program's policies and contractual requirements for facial technology vendors, the FTC

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

did not seek civil penalties, and imposed a no-money, no-fault order. The case helpfully articulates what the FTC deems as “best practices” for the use of facial recognition technologies, including the usage of cameras and smartphones by retailers to detect and stop shoplifting and to mitigate risks of misidentification. **e. Financial Privacy** The FTC approved further changes to its Standards for Safeguarding Customer Information Rule (“Safeguards Rule”) in 2023. The Safeguards Rule requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain a comprehensive security program to keep their customers’ information safe. The rule was initially amended in October 2021 in response to “widespread data breaches and cyberattacks” by introducing more robust data security requirements for financial institutions to protect their customers’ data.[112] In 2023, the FTC further amended the rule to require financial institutions to report certain data breaches directly to the FTC.[113] Many provisions of the 2021 rule changes went into effect on January 10, 2022, but certain provisions of the Safeguards Rule did not take effect until June 9, 2023.[114] These sections require financial institutions to:

- Designate a qualified individual to oversee their information security program;
- Develop a written risk assessment;
- Limit and monitor who can access sensitive customer information;
- Encrypt all sensitive information;
- Train security personnel;
- Develop an incident response plan;
- Periodically assess the security practices of service providers; and
- Implement multifactor authentication or another method with equivalent protection for any individual accessing customer information.[115]

The FTC’s 2023 amendments include more specific criteria for what safeguards financial institutions must implement as part of their information security program, and requirements to explain their information-sharing practices and designate a single qualified individual to oversee their information security program and report periodically to an organization’s board of directors, or a senior officer in charge of information security.[116] These amendments will not take effect until mid-2024. **f. Children’s and Teens’ Privacy** On December 20, 2023, the FTC announced long-awaited proposed amendments to the Children’s Online Privacy Protection Rule (“COPPA Rule”).[117] If adopted, the proposed amendments would be the first changes to the COPPA Rule in a decade.[118] The amendments aim to modernize the COPPA framework and shift the burden for protecting children’s privacy and security from parents to service providers.[119] The proposed changes include:

- Requiring separate opt-in for targeted advertising;
- Prohibiting conditioning a child’s participation on collection of personal information;
- Limiting the support for the internal operations exception, which allows operators to collect persistent identifiers without first obtaining verifiable parental consent as long as the operator does not collect any other personal information;
- Imposing restrictions on educational technology companies, including prohibiting these companies’ use of students’ data for commercial purposes;
- Increasing accountability for Safe Harbor programs, including by requiring each program to publicly disclose its membership list and report additional information to the Commission;
- Strengthening data security requirements; and
- Limiting data retention.[120]

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

The FTC also recently sought comments from the Entertainment Software Rating Board and others for a new mechanism for obtaining parental consent under the COPPA Rule: "Privacy-Protective Facial Age Estimation" technology, which analyzes the geometry of a user's face to accurately confirm a user's age.[121] The FTC's request for comments focused on whether such age verification methods would satisfy the COPPA Rule's requirements and whether it poses a privacy risk to children's biometric and other personal information.[122] In 2023, the FTC pursued enforcement action against major technology companies in relation to children's and teen's' privacy. For example, the FTC alleged a technology company violated the COPPA Rule by collecting and illegally retaining personal information from children who signed up for a gaming service without parental consent.[123] The company agreed to pay $20 million and take steps to increase privacy protection for children users to settle the case.[124] The FTC has also proposed changes to its 2020 order with another technology company, alleging in part that the company has not fully complied with the order because it misled parents about their ability to control with whom their children communicated.[125] Among other things, the proposed changes would prohibit the company from monetizing data it collects from users under 18.[126] **g. Biometric Information** On May 18, 2022, the FTC signaled an increased focus on preventing the misuse of biometric information in a policy statement.[127] The policy statement is a first-of-its-kind comprehensive breakdown of the FTC's view that the commercial use of biometric information poses certain privacy risks to consumers, and it builds on prior workshops and statements analyzing consumer protection issues related to specific technologies that can implicate biometric information.[128] In the policy statement, the FTC broadly defines biometric information as data depicting or describing a person's physical, biological, or behavioral traits, characteristics, or measurements, including facial features, iris or retina, fingerprints or handprints, voice, genetics, or characteristic movements or gestures.[129] The FTC warned that certain conduct relating to the use of biometric information and biometric information technologies constitutes an unfair or deceptive practice under Section 5 of the FTC Act, including:

- Making false or unsubstantiated marketing claims regarding the validity, reliability, accuracy, performance, fairness, or efficacy of technologies relying on biometric information;
- Making deceptive statements about the collection and use of biometric information;
- Failing to protect consumers' biometric information using reasonable data security practices;
- Collecting biometric information that consumers meant to conceal or keep private (including by implementing "privacy-invasive default settings");
- Selling technologies that permit harmful or illegal conduct, such as covert tracking; and
- Using or selling discriminatory technologies.[130]

To avoid liability under the FTC Act, the FTC recommends that businesses communicate the use and capabilities of biometric information technologies to consumers, ensure biometric information technologies operate fairly and accurately, and implement safeguards to prevent unauthorized access to biometric information. Relying on the policy statement for the first time, the FTC filed a complaint in December 2023 alleging that a drugstore chain surreptitiously used facial recognition technology to identify—sometimes falsely—shoplifters and other customers it deemed problematic, as described above.[131] **2. Consumer Financial Protection Bureau** Notwithstanding increasing congressional antagonism directed at the Consumer Financial Protection Bureau ("CFPB"), the CFPB did not decrease its attention on privacy issues in 2023. Last year, the CFPB issued a long-awaited proposed rule regarding consumer personal financial data rights and signaled an intent to increase its oversight of non-bank entities providing digital wallets and peer-to-peer apps, as well as data brokers that sell certain types of consumer data. The CFPB also parroted the FTC's concerns with privacy risks associated with AI. **a. Personal Financial Data Rights Rulemaking** On October 19, 2023, the CFPB released a long-

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

awaited Notice of Proposed Rulemaking on Personal Financial Data Rights.[132] If adopted, this rule would establish a regulatory framework where consumers have the power "to break up with banks that provide bad service and would forbid companies that receive data from misusing or wrongfully monetizing the sensitive personal financial data."[133] The proposed rule would also require covered financial entities to share a consumer's financial data with authorized third parties upon the consumer's request.[134] The proposed rule is the first proposal to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"), which authorizes the CFPB to prescribe rules under which consumers may access information about themselves from their financial service providers.[135] Although Section 1033 applies to all consumer financial products or services covered under the Dodd-Frank Act,[136] the proposed rule would limit the scope of covered entities, or "data providers," to Regulation Z card issuers, Regulation E financial institutions, and other payment facilitation providers, while generally exempting data providers that do not have a consumer interface.[137] Under the proposed rule, data providers must provide consumers and authorized third parties with "covered data," such as transaction information, account balance, and upcoming bill information, "in an electronic form usable by consumers and authorized third parties," as provided by Section 1033 of the Dodd-Frank Act.[138] In addition to requiring third parties to obtain "express informed consent" from the consumer to become authorized to access covered data, the proposed rule would also prohibit such authorized third parties from collecting, using, or retaining the consumer's relevant data beyond what is "reasonably necessary" to provide the requested product or service to a consumer.[139] The proposal does not define what is "reasonably necessary," but instead enumerates activities that do not qualify: (i) targeted advertising; (ii) cross-selling of other products or services; or (iii) the sale of covered data.[140] The proposed rule also imposes data accuracy and data security obligations, among other obligations, on authorized third parties.[141] The comment period for the proposed rule closed on December 29, 2023; CFPB Director Rohit Chopra said that the agency intends to finalize the rule by fall 2024.[142] **b. Increased Oversight of Non-bank Entities** On November 7, 2023, the CFPB issued a proposed rule that, if adopted, would establish supervisory power over big technology firms and other nonbank entities that offer services allowing consumers to digitally transfer money.[143] The proposed rule would apply to "larger participant" nonbank entities that handle more than five million payment transactions per year through digital wallets, peer-to-peer apps, payment apps, and other "covered payment functionalities."[144] This oversight authority would allow the CFPB to conduct examinations to ensure that these nonbank entities are adhering to applicable laws governing funds transfer, privacy, and consumer protection.[145] The comment period for this proposed rule closed on January 8, 2024.[146] **c. Increased Scrutiny of Data Brokers** In March 2023, the CFPB launched an inquiry into data brokers to inform whether existing Fair Credit Reporting Act ("FCRA") rules reflect the market realities of "[m]odern data surveillance practices [that] have allowed companies to hover over our digital lives and monetize our most sensitive data."[147] The agency's request for information defined "data brokers" broadly as "an umbrella term to describe firms that collect, aggregate, sell, resell, license, or otherwise share consumers' personal information with other parties."[148] That definition could sweep in companies, like credit unions and banks, that are not typically considered data brokers. On August 15, 2023, Director Chopra also announced that the CFPB will be developing new rules that define a data broker that sells certain types of consumer data as a "consumer reporting agency" ("CRA") under FCRA.[149] Defining data brokers as CRAs would impose new obligations on data brokers to comply with FCRA's demanding standards for data accuracy and privacy, including consumer access and consent rights.[150] Director Chopra also announced a second proposal under consideration that will clarify the extent to which credit header data, such as name, date of birth, and social security number, constitute a consumer report, and thereby limit the ability of CRAs to impermissibly disclose identifying contact information.[151] The CFPB intends to propose these changes for public comment in 2024.[152] **d. Artificial Intelligence and Algorithmic Bias** In an April 25, 2023 joint statement with the DOJ, FTC, and Equal Employment Opportunity Commission, the CFPB reaffirmed its commitment to enforce consumer financial protection laws to prevent harmful uses of AI and algorithmic bias.[153] Since then, the CFPB has highlighted risks

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

associated with AI in multiple contexts: ***Chatbots*.** In June 2023, the CFPB released an issue spotlight on the risks associated with the use of chatbots by financial institutions, including consumer financial protection compliance risks and failures to protect consumer privacy and data, diminished trust and customer service, and harm to consumers resulting from inaccurate information.[154] ***Home Appraisals*.** In June 2023, the CFPB also proposed a rule that would govern automated home valuations.[155] The rule would require institutions that employ automated valuation models to take certain steps to minimize inaccuracy and bias by adopting policies, practices, procedures, and control systems to ensure that models adhere to quality control standards designed to ensure a high level of confidence in the estimates produced.[156] Under the proposal, institutions would also be required to protect against the manipulation of data, seek to avoid conflicts of interest, require random sample testing and reviews, and comply with applicable nondiscrimination laws.[157] The public comment period ended on August 21, 2023.[158] ***Credit Decisions.*** In September 2023, the CFPB issued a Consumer Protection Circular titled "Adverse Action Notification Requirements and the Proper Use of the CFPB's Sample Forms Provided in Regulation B," concerning lenders' obligations when using AI to make consumer credit decisions.[159] The guidance emphasizes that creditors must provide accurate and specific reasons for adverse decisions made by complex algorithms, and this requirement is not automatically satisfied by use of a sample adverse action checklist.[160] **3. Securities and Exchange Commission** In 2023, the SEC continued to focus on transparency around cybersecurity risk management and incident disclosure, as made evident by the Commission's rulemaking and enforcement activity. Most notably, the SEC finalized rules requiring public companies to report material cybersecurity incidents within four business days of determining materiality, as well as periodic disclosures relating to cybersecurity risk management, strategy, and governance. The SEC was also active on the enforcement front, pursuing actions against companies and individuals in connection with cyber incidents. In 2024, we expect to see heightened enforcement activity as the newly adopted cyber rules take effect and as the SEC takes final action on proposed rulemaking for registered entities, particularly those implicating personal information or sensitive data. **a. Regulation March 2023 – SEC Proposes Rules to Amend Regulation S-P** On March 15, 2023, the SEC proposed rules that would amend Regulation S-P to update and close certain gaps in the requirements pertaining to the protection of customer information.[161] Most importantly, if adopted, the amendments would require broker-dealers, investment companies, registered investment advisers, and transfer agents ("Covered Institutions") to adopt written policies and procedures for responding to unauthorized access to or use of customer information.[162] The amendments would also require Covered Institutions to notify individuals of unauthorized use of or access to their sensitive information "as soon as practicable," but not later than 30 days, after discovery of a data breach.[163] As explained in the adopting release, the rules would also amend other aspects of Regulation S-P, including:

- Extending the protections of the safeguards and disposal rules to both nonpublic personal information that a Covered Institution collects about its own customers and to nonpublic personal information that a covered institution receives about customers of other financial institutions;
- Extending the safeguards rule, as amended, to registered transfer agents, and expanding the disposal rule to include transfer agents registered with another appropriate regulatory agency; and
- Conforming Regulation S-P's existing provisions relating to the delivery of an annual privacy notice for consistency with a statutory exception created by Congress in 2015.[164]

The public comment period closed on June 5, 2023, but the SEC has not indicated whether and when it will take final action on the proposed amendments. **July 2023 – SEC Adopts New Cybersecurity Disclosure Rules for Public Companies** On July 26, 2023, as reported in Gibson Dunn's client alert, the SEC adopted a final rule to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

SEC Act of 1934 (the “Exchange Act”).[165] The final rule requires: (i) Form 8-K disclosure of material cybersecurity incidents within four business days of the company’s determination that the cybersecurity incident is material; and (ii) annual disclosures in Form 10-K regarding the company’s cybersecurity risk management, strategy, and governance.[166] For foreign private issuers, the final rule amends Form 20-F to include requirements parallel to Item 106 regarding risk management, strategy, and governance.[167] In addition, the final rule adds “material cybersecurity incidents” to the items that may trigger a current report on Form 6-K.[168] Under the new rule, foreign private issuers will be required to furnish on Form 6-K information about material cybersecurity incidents that the issuers disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders.[169] Compliance Dates The Form 8-K disclosure requirement went into effect on December 18, 2023 for most registrants (smaller companies will have until June 5, 2024 to comply); all registrants will have to comply with the annual disclosure requirements beginning with their Form 10-K or 20-F filing for the fiscal year ending on or after December 15, 2023.[170] Reporting Material Cybersecurity Incidents Under the final rules, when a company experiences a material cybersecurity incident, it must disclose on Form 8-K, the material aspects of the nature, scope, and timing of the incident, and the material impact or “reasonably likely” material impact on the company, including on its financial condition and results of operations.[171] Importantly, this disclosure must be made within four business days of the company determining that it has experienced a material cyber incident, a determination which must be made “without unreasonable delay after discovery of the incident.”[172] In circumstances where a company has determined that a cybersecurity incident is material but does not have all of the information that is required to be disclosed when the Form 8-K filing is due, the company must later update the disclosure through a Form 8-K amendment.[173] The final rule permits companies to delay reporting material cyber incidents up to an initial period of 30 days, if the U.S. Attorney General notifies the SEC in writing that immediate disclosure would pose a substantial risk to national security or public safety.[174] However, as confirmed by guidelines released by the Department of Justice,[175] the Attorney General will only permit delayed disclosures in very limited circumstances, so public companies should be prepared to disclose virtually all material cyber incidents within four days after determining materiality.[176] The DOJ guidelines also make clear that even where the Attorney General grants a delay, the delay may not delay filing the Form 8-K in its entirety, but may only pertain to some of the information that is required to be disclosed.[177] **Annual Reporting Requirements** The final rule also requires that public companies include on their Form 10-K filings certain disclosures regarding the company’s cybersecurity risk management, strategy and governance.[178] The final rule also includes parallel requirements for a foreign private issuer’s risk management, strategy, and governance disclosures on Form 20-F.[179] *Risk management strategy and governance disclosure.* Companies are required to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes, including information regarding:

- Whether and how any such processes have been integrated into the company’s overall risk management system or processes;
- Whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
- Whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.[180]

Public companies are also required to describe whether and how any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition.[181] Notably, the final rule requires disclosure of “processes” (as opposed to “policies and procedures”) in order to avoid requiring disclosure of operational details that could be exploited by threat actors

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

and make clear that companies without written policies and procedures need not disclose that fact. *Governance Disclosures.* The final rule also requires public companies to describe on Form 10-K how the board of directors oversees the company's cybersecurity risks. This includes identifying, if applicable, any board committee or subcommittee responsible for the oversight of cybersecurity risks and describing the processes by which the board or such committee is informed about such risks.[182] Additionally, companies must describe management's role in assessing and managing the company's material cybersecurity risks from cybersecurity.[183] **September 2023 – SEC Approves Revised Privacy Act Rule** On September 20, 2023, the SEC approved a final rule, adopting amendments to the SEC's regulations under the Privacy Act of 1974, which governs the federal government's handling of personal information.[184] The final rule updates and streamlines the SEC's Privacy Act regulations, including the process for submitting and receiving responses to Privacy Act requests and administrative appeals and provides electronic methods to verify an individual's identity.[185] Given the extensive nature of the amendments, the final rule replaces entirely the current version of the Privacy Act regulations which was last updated in 2011. The final rule went into effect on October 26, 2023. **Cyber Rules for Registered Investment Advisers, Registered Investment Companies, and Business Development Companies Expected in April 2024.** In February 2022, the SEC proposed cybersecurity rules for registered investment advisers, registered investment companies, and business development companies (the "RIA Rules").[186] If adopted, the RIA Rules would require covered companies to, among other things, (i) adopt written cybersecurity policies and procedures to address cybersecurity risk, and (ii) report significant cybersecurity incidents, which are those that "significantly affect the critical operations" of a covered company or lead to "unauthorized access or use of information that results in substantial harm" to a covered company, or its clients, funds, or investors.[187] As noted on the SEC's June 13, 2023 rulemaking agenda, the RIA Rules have entered the final rule stage[188] and are expected to be finalized in April 2024.[189] Looking ahead, the SEC Division of Examinations announced its priorities for 2024, which stated that it plans to continue focusing on "registrant's policies and procedures, internal controls, oversight of third-party vendors (where applicable), governance practices, and responses to cyber-related incidents."[190] SEC Chair Gary Gensler emphasized that the "Division's efforts, as laid out in the 2024 priorities, enhance trust in our ever-evolving markets."[191] Information security and cybersecurity will remain a key area of regulation and enforcement for the SEC in 2024. **b. Enforcement** In addition to new rules, in 2023 the SEC continued to pursue enforcement actions at a historically high level against public companies, investment firms, law firms, and individuals.[192] The SEC obtained orders totaling nearly $5 billion in financial remedies in fiscal year 2023, the second-highest amount in SEC history following a record-setting nearly $6.5 billion in fiscal year 2022.[193] Notably, the SEC continued to focus on individuals, with about two-thirds of the SEC's cases in fiscal year 2023 involving individuals.[194] The SEC also obtained orders that barred 133 individuals from serving as officers or directors for public companies, the highest such number in a decade.[195] We expect these trends to continue in 2024, particularly as they relate to cybersecurity when the SEC's newly adopted cyber rules take effect and additional cyber rules are finalized. Below is a summary of some of the most notable cyber-related enforcement actions brought by the SEC in 2023. ***Broker-Dealer Username/Password Handling Litigation.*** In September, 2023, the SEC alleged that a broker-dealer and its parent company allegedly made materially false and misleading statements and omissions regarding information barriers intended to prevent the misuse of sensitive customer information.[196] The SEC alleged that the broker-dealer operated two businesses that were purportedly walled off from each other by data safeguards: a trade order execution service for institutional customers that typically operated on commission, and a proprietary trading business. However, during a 15-month period from 2018 to 2019, the broker-dealer allegedly failed to adequately safeguard a database of post-trade information regarding customer orders that included customer identifying information and further material nonpublic information.[197] The broker-dealer allegedly rendered the database accessible to virtually anyone at its affiliates by leaving the data accessible via "two sets of widely known and frequently shared generic usernames and passwords."[198] The SEC asserts that this alleged failure to safeguard the information posed significant risk that proprietary traders could abuse it or

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

distribute it outside the entity.[199] The litigation remains pending. ***Settlement for Allegedly Misleading Statements Related to 2020 Ransomware Attack.*** In March 2023, the SEC imposed a $3 million civil penalty to settle allegations it brought against a public company for making allegedly misleading disclosures concerning a 2020 ransomware attack that had impacted over 13,000 customers.[200] The SEC alleged that, on July 16, 2020, the company announced a ransomware attacker had not gained access to customer bank account information or Social Security Numbers.[201] Within days of the announcement, however, technology and customer relations personnel allegedly learned that the attacker had accessed and exfiltrated that sensitive information.[202] The employees nonetheless allegedly failed to communicate this information to senior management accountable for its public disclosure because, in the SEC's view, the company failed to maintain adequate disclosure controls and procedures.[203] As a result, the company's 10-Q report filed in August 2020 did not include this information about the cyberattack, which the SEC views as an omission of material information. In addition, the SEC alleged that the company's description of the risk of disclosure of sensitive customer information as a hypothetical risk was misleading.[204] ***SEC Alleges Fraud Against Public Company and its CISO.*** In October 2023, the SEC alleged that a network monitoring software company and its Chief Information Security Officer ("CISO") engaged in fraud and internal controls violations.[205] The SEC alleges that the company and its CISO overstated its cybersecurity practices and understated or failed to disclose known cybersecurity risks.[206] The SEC's complaint alleges that the company's public statements conflicted with its internal assessments.[207] The complaint also alleges that the CISO was aware of the company's cybersecurity risks, but failed to resolve the issues or sufficiently elevate them.[208] The SEC alleged that the cybersecurity shortfalls rendered the company unable to provide reasonable assurances that its most valuable assets were sufficiently protected.[209] The lapses in cybersecurity practices allegedly resulted in a two-year cyberattack campaign against the software company and some of its customers, including federal and state government agencies.[210] The cyberattack was first disclosed publicly in December 2020, though the SEC alleged that disclosure was incomplete.[211] According to the SEC, the company and CISO allegedly "paint[ed] a false picture of the company's cyber controls environment."[212] The SEC alleged that the company and CISO violated antifraud provisions of the securities laws, that the company violated reporting and internal controls provisions, and that the CISO aided and abetted the company's violations.[213] The SEC seeks permanent injunctive relief, disgorgement with prejudgment interest, civil penalties, and an officer-and-director bar against the CISO.[214] Going forward, we expect to see a significant uptick in enforcement activity, particularly around cybersecurity disclosures, given the adoption of the SEC's cyber disclosure rules which went into effect in December 2023 and other proposed cyber rules pending finalization, as discussed above. **4. Department of Health and Human Services and HIPAA** On February 27, 2023, the Department of Health and Human Services ("HHS") announced three new divisions within the Office of Civil Rights ("OCR"): an Enforcement Division, a Policy Division, and a Strategic Planning Division.[215] OCR enforces HIPAA and the Health Information Technology for Economic and Clinical Health Act of 2009, among additional privacy-related and other statutes.[216] OCR explained that its caseload has increased 69 percent from 2017 and 2022.[217] OCR thus created the new divisions to "improve[] OCR's ability to effectively respond to complaints, put[ting] OCR in line with its peers' structure and mov[ing] OCR into the future."[218] The addition of three new divisions in OCR signals and underscores the heightened importance of data privacy and security within HHS. **a. Rulemaking on HIPAA Compliance and Data Breaches** On December 13, 2023, HHS finalized a rule implementing the 21st Century Cures Act that enhances the Office of the National Coordinator for Health Information Technology Certification Program, aimed at advancing interoperability, transparency, and the access, exchange, and use of electronic health information.[219] The final rule is designed to increase algorithm transparency and information sharing for healthcare providers.[220] The provisions of the rule are based on the principles of "fairness, appropriateness, validity, effectiveness and safety," and include certification criteria for "decision support interventions," "patient demographics and observations," "electronic case reporting," and the "exchange and use" of electronic health information.[221] The final rule goes into effect on February 8, 2024.[222] **b. Telehealth and Data Security**

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Guidance HHS released a fact sheet in early 2023 identifying what will change as a result of the expiration of the federal Public Health Emergency for COVID-19 on May 11, 2023.[223] HHS stated that the "vast majority" of current Medicare telehealth flexibilities (such as waivers of geographic and originating site restrictions and the allowance of audio-only telehealth services) will remain in place through December 2024.[224] The agency also made some Medicare changes permanent so that they will stay in place now that the public health emergency has ended. These include allowing Federally Qualified Health Centers and Rural Health Centers to "serve as a distant site provider for behavioral/mental telehealth services," allowing Medicare patients to "receive telehealth services for behavioral/mental health care in their home," and allowing "behavioral/mental telehealth services" to "be delivered using audio-only communication platforms."[225] On July 20, 2023, the FTC and HHS issued a joint letter to 130 hospital systems and telehealth providers, warning them to "exercise extreme caution" with respect to certain online technologies that are incorporated in their websites and apps given the potential privacy risks these technologies may pose to patient data.[226] The letter also reminded healthcare providers about their obligations under HIPAA and the FTC's Health Breach Notification Rule.[227] Relatedly, on September 15, 2023, the FTC and HHS issued an updated publication addressing businesses' potential questions related to collecting, using, and sharing consumer health information, and provided links to more detailed guidance.[228] **c. Reproductive and Sexual Health Data** On June 24, 2023, HHS Secretary Xavier Becerra released a statement[229] on the one-year anniversary of *Dobbs v. Jackson Women's Health Org.*, which reversed *Roe v. Wade* and ended federal protection for abortion access.[230] The statement highlights HHS's efforts to protect and expand access to reproductive care, and outlines three "priority areas":

1. "Reaffirming the Department's commitment to protecting the right to abortion care in emergency settings under the Emergency Medical Treatment and Labor Act (EMTALA)";
2. "Clarifying protections for birth control coverage under the Affordable Care Act"; and
3. "Protecting medical privacy – including empowering patients to protect their medical information on smart phones, apps, and other platforms."[231]

On April 12, 2023, HHS proposed measures to strengthen patient-provider confidentiality related to reproductive health care through a Notice of Proposed Rulemaking for the Privacy Rule.[232] The proposed rule would prohibit the use or disclosure of protected health information ("PHI") to identify, investigate, sue, or prosecute "patients, providers, and others involved in the provision of legal reproductive health care, including abortion."[233] The public comment period closed on June 16, 2023; and the proposed rule is expected to be finalized in March 2024.[234] **d. HHS Enforcement Actions** OCR continued to enforce the HIPAA Privacy Rule throughout 2023, which has been a continued focus of the agency in recent years. For example, OCR settled claims against a New York-based non-profit academic medical center for alleged violations in 2020 of the HIPAA Privacy Rule.[235] A national newspaper published an article about the medical center's COVID-19 emergency response, "which included photographs and information about the facility's patients" exposing patient information, including COVID-19 diagnoses, medical statuses and prognoses, vital signs, and treatment plans.[236] OCR alleged that the facility disclosed three patients' protected health information to the press "without first obtaining written authorization from the patients."[237] The settlement required the facility to pay $80,000 and agree to implement a corrective action plan "to develop written policies and procedures that [complied] with the HIPAA Privacy Rule."[238] HHS also focused its enforcement efforts around the HIPAA Right of Access Initiative, which was launched in 2019 and requires covered entities to provide individuals with "timely access to their health information for a reasonable cost" under the HIPAA Privacy Rule.[239] As of December 15, 2023, OCR had brought 46 cases pursuant to the HIPAA Right of Access Initiative.[240] These actions were largely brought against covered entities for failing to provide individuals with copies of protected health information within the required timeframe and/or in accordance with permitted fees.[241] Data breaches have been

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

another recent priority. In February 2023, a nonprofit health system in Arizona agreed to pay $1.25 million to resolve alleged HIPAA Security Rule violations arising from a 2016 data breach, which disclosed the protected health information of 2.81 million individuals.[242] In addition to the monetary penalty, the hospital system agreed to implement a corrective action plan, and two years of OCR monitoring, to address alleged deficiencies relating to the protection of electronic PHI, including pertaining to risk assessment, vulnerability management, monitoring, authentication and protection of data transit.[243] In December 2023, OCR also entered into a settlement with a Louisiana-based medical group for $480,000, stemming from a phishing attack that exposed the personal information of over 34,000 individuals.[244] OCR alleged that the group failed to conduct a risk analysis of potential vulnerabilities, as required under HIPAA.[245] As with Banner Health, Lafourche agreed to implement a corrective action plan that OCR will monitor for two years [246] **5. Other Federal Agencies a. Department of Homeland Security** In 2023, the Department of Homeland Security ("DHS") continued to pursue various cybersecurity initiatives aimed at securing critical infrastructure and helping organizations respond to the rapidly evolving cyber threat landscape. The year marked an increased focus on cyber incident information sharing and reporting through public-private and cross-border partnerships. On March 2, 2023, DHS Secretary Alejandro N. Mayorkas released a statement about working to implement President Biden's National Cybersecurity Strategy and emphasized the role of public-private sector collaboration and work with DHS's Cyber Safety Review Board and Cybersecurity and Infrastructure Security Agency ("CISA").[247] As required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), DHS and the Cyber Incident Reporting Council issued recommendations to Congress for streamlining the reporting of cyber incidents by establishing standard definitions, timelines, and triggers for reporting; creating a model incident reporting form for federal agencies; and creating a central reporting web portal.[248] These recommendations will inform CISA's ongoing rulemaking process, as it works towards publishing a Notice of Proposed Rulemaking related to CIRCIA's reporting requirements by March 2024.[249] Secretary Mayorkas also hosted cyber leaders from 21 nations at the Western Hemisphere Cyber Conference to discuss bilateral and multilateral initiatives to respond to, and facilitate increased information sharing about, cybersecurity challenges, including around critical infrastructure and cyber-enabled crimes and ransomware.[250] DHS also released multiple reports and advisories outlining recommendations to mitigate risks posed by threat actor groups and vulnerabilities affecting critical infrastructure, including malware attacks by the ransomware group CL0P against users of certain file-transfer software;[251] targeting of industry-standard security tools by threat actor group Lapsus$;[252] and a ransomware variant used to exploit a vulnerability that threatened critical infrastructure.[253] DHS also increased its State and Local Cybersecurity Grant Program funding from $185 million in FY22 to $374.9 million in FY23, signaling the growing importance of protecting communities from cyber threats.[254] **b. Department of Justice** In 2023, DOJ continued to focus on and expand its capacity to address cyber threats, especially those related to national security. In a series of press releases, DOJ touted certain accomplishments in its ongoing fight against organized cybercrime. For example, it publicized actions it had taken against several ransomware groups, including the Hive and Blackcat, as well as the malware code Qakbot. DOJ also announced significant developments regarding its approach to the issue of algorithmic bias, including an innovative resolution reached with a large social media company and the filing of a statement of interest in a case alleging racial discrimination against rental applicants. As part of its continued and expanding efforts to counter cyber-related national security threats arising from nation-state actors, DOJ created the National Security Cyber Section ("NatSec Cyber") within the National Security Division ("NSD").[255] DOJ noted that NatSec Cyber "will allow NSD to increase the scale and speed of disruption campaigns and prosecutions of nation-state threat actors, state-sponsored cybercriminals, associated money launderers, and other cyber-enabled threats to national security."[256] DOJ continued its aggressive, multifaceted efforts to disrupt domestic and international organized cybercrime via collaboration between the FBI and foreign law enforcement organizations. For example, in January 2023, DOJ announced that its months-long campaign against a ransomware-as-a-service network called the "Hive" culminated in the seizure of thousands of decryption keys that were then distributed to victims of the Hive's

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

activities, as well as the shutting down of servers and websites used by the Hive to coordinate attacks.[257] The Hive's ransomware campaign impacted more than 1,500 victims, "including hospitals, school districts, financial firms, and critical infrastructure," across more than 80 countries, and sought to extort hundreds of millions of dollars in ransomware payments.[258] In May 2023, DOJ publicized an operation code-named "MEDUSA," which involved the deployment of an FBI-developed tool named "PERSEUS" to disrupt the ability of the highly sophisticated cyber espionage malware named "Snake" to compromise infected computers.[259] Snake, whose development the U.S. government attributes to a unit in the Federal Security Service of the Russian Federation, has been used and adapted for the last nearly 20 years to steal and covertly transfer sensitive information from computer networks in over 50 countries, often in service of Russian interests.[260] In August 2023, DOJ announced another multinational effort to degrade and avert attacks from Qakbot, a malware code used by cybercriminals to create malicious botnets and perpetrate "ransomware, financial fraud, and other cyber-enabled criminal activity."[261] Finally, in December 2023, DOJ announced that the FBI had successfully built a decryption tool that allowed victims of the ransomware-as-a-service group Blackcat (also known as ALPHV or Noberus) to regain control of their systems.[262] This was in addition to taking control of websites associated with the group, which had previously carried out attacks targeting "government facilities, emergency services, defense industrial base companies, critical manufacturing, and healthcare and public health facilities—as well as other corporations, government entities, and schools," costing victims hundreds of millions of dollars in ransom payments, incident response costs, and losses from data damage and theft.[263] DOJ also waded into issues around algorithmic bias. In January 2023, for example, DOJ announced a resolution reached with a large social media company to address alleged algorithmic bias on its platforms.[264] This development came as part of a settlement stemming from a June 2022 lawsuit filed in the U.S. District Court for the Southern District of New York that asserted the company engaged in discriminatory delivery of housing advertisements based on algorithms partially relying on protected characteristics in violation of the Fair Housing Act ("FHA").[265] The settlement agreement required the company to create a system (dubbed the Variance Reduction System) to promote the "equitable distribution of ads" across its platforms, subject to certain compliance metrics, oversight by the court, and ongoing monitoring by a third-party reviewer through June 27, 2026.[266] A DOJ official praised the agreement and the company for setting "a new standard for addressing discrimination through machine learning" and called for others to follow the company's lead. DOJ also filed a Statement of Interest in an FHA case pending in a Massachusetts federal district court brought by two Black rental applicants alleging unlawful algorithmic tenant screening practices.[267] Plaintiffs alleged that the screening system discriminated "against Black and Hispanic rental applicants in violation of the FHA."[268] According to DOJ, the Statement confirms its "commitment to ensuring that the Fair Housing Act is appropriately applied in cases involving algorithms and tenant screening software."[269] **c. Department of Commerce**
On March 7, 2023, a bipartisan group of senators proposed the Restricting the Emergence of Security Threats that Risk Information and Communications Technology ("RESTRICT") Act, which would give the Commerce Secretary the power to ban foreign?owned technologies if they are found to pose national security threats.[270] The bill, which received support from the Department of Commerce,[271] was referred to the Committee on Commerce, Science, and Transportation, and is currently awaiting further action.[272] On June 14, 2023, Senator Wyden introduced the Protecting Americans' Data From Foreign Surveillance Act of 2023, which would update the Protecting Americans' Data From Foreign Surveillance Act of 2022 that was introduced in June 2023 but not passed.[273] This bill would bar exports of sensitive data to high?risk countries, as determined by the Department of Commerce.[274] The Department of Commerce would also be tasked with defining sensitive data, though the bill broadly covers data, including browsing history and location data.[275] However, the new export rules would not apply to data encrypted with technology approved by the National Institute of Standards and Technology ("NIST").[276] The bill was referred to the Committee on Banking, Housing, and Urban Affairs, and currently awaits further progress.[277] **d. Department of Energy**
Through the Infrastructure Investment and Jobs Act, the Department of Energy ("DOE") has provided significant funding to a series of new cybersecurity programs.[278] On

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

September 12, 2023, the DOE announced $39 million of funding for nine new “National Laboratory” projects to strengthen the cybersecurity of distributed energy resources (“DER”).[279] The funding is intended to “support targeted research, development, and demonstration related to different elements of the DER landscape.”[280] Despite investing in improved cybersecurity for DER, the DOE itself continues to attract scrutiny of its cybersecurity practices, especially from the DOE’s Office of Inspector General (“OIG”). Ongoing concerns regarding the department’s cybersecurity capabilities stem in part from three apparent cyberattacks against DOE national laboratories in late 2022, which were serious enough to prompt House lawmakers to seek details concerning them in early 2023.[281] In November 2023, the OIG released a report discussing “management challenges” at the DOE, including numerous cybersecurity-related deficiencies.[282] In discussing these deficiencies, the report noted structural and resource-based challenges to an effective organization-wide cybersecurity program, some of which stemmed from inconsistent and outdated practices by DOE contractors.[283] Thus, contractors/vendors doing business with the DOE should expect a greater emphasis on and scrutiny of their cybersecurity practices going forward. **e. Department of Defense** In December 2023, the Department of Defense (“DoD”) released a proposal designed to implement its Cybersecurity Maturity Model Certification (“CMMC”) program, broadly aimed at increasing the security of controlled, unclassified information across the defense industry.[284] The CMMC will set three “levels” of cybersecurity requirements based on the nature of information held by contractors, while ultimately creating a baseline level of cybersecurity for almost all DoD contract solicitations.[285] The program will be implemented in phases over several years, giving companies time to study and understand its requirements and prepare staff to comply with them.[286] **f. Federal Communications Commission** The Federal Communications Commission (“FCC”) was particularly focused on the Telephone Consumer Protection Act (“TCPA”) and cybersecurity issues in 2023. In June 2023, the FCC unveiled a new Privacy and Data Protection Task Force that will “coordinate across the agency on the rulemaking, enforcement, and public awareness needs in the privacy and data protection sectors.”[287] The task force will address issues such as data breaches of telecommunication providers linked to cyber intrusions and supply chain vulnerabilities.[288] ***TCPA Rulemaking*.** In January 2023, the FCC announced that new rules promulgated under Section 8 of the Telephone Robocall Abuse Criminal Enforcement and Deterrence (“TRACED”) Act[289] would go into effect on July 20, 2023.[290] Among other things, the FCC’s new rules provide additional clarity on exemptions from the TCPA, including establishing limits on the number of exempt calls that can be made to a residence during a 30-day period (for non-commercial, non-advertising, or nonprofit purposes); requiring callers to obtain consent before exceeding the numerical limits on exempt calls; and mandating ways that consumers can opt out of exempted calls to residential lines.[291] In the last quarter of 2023, the FCC took additional regulatory steps to curb robocalls. On October 23, 2023, FCC Chairwoman Jessica Rosenworcel announced the FCC was opening an inquiry into the impact of artificial intelligence technology on robocalls, particularly for more vulnerable consumers such as seniors and those on fixed incomes.[292] Following that announcement, the FCC sought public input to better understand the impact of emerging AI technologies on unwanted telephone calls and text messages.[293] It seems likely that the FCC will continue to assess AI’s impact in this area. On December 18, 2023, the FCC also approved new TCPA rules that require 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.[294] The rule is intended to end companies’ prior practice of relying on a single consent to receive automated calls from multiple marketing partners. The new rule has closed this loophole, and requires one-to-one consent for each marketing partner.[295] There will be an implementation period of at least 12 months to allow companies to make necessary changes to ensure consent complies with the new rules.[296] ***Cyber Trust Mark.*** In July 2023, the FCC, in coordination with the White House, announced a proposal to create a “U.S. Cyber Trust Mark” label for devices that meet certain cybersecurity and privacy criteria set by the National Institute of Standards and Technology, with voluntary commitments to the standard to be made by manufacturers and retailers.[297] Examples of contemplated features offered by labeled

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

devices include “unique and strong default passwords, data protection, software updates, and incident detection capabilities.”[298] In August 2023, the FCC released a Notice of Proposed Rulemaking regarding the proposal to collect public input, noting that if it votes to establish the program, it could be “up and running” by late 2024.[299] ***VoIP and TRS Rules.*** In December 2023, the FCC approved modifications to data breach notification rules for providers of telecommunications, interconnected Voice over Internet Protocol (“VoIP”), and telecommunications relay services (“TRS”).[300] The modifications expand reportable personally identifiable information and the definition of a “breach,” and require carriers or TRS providers to notify the FCC of breaches, in addition to other existing reporting requirements.[301] ***Enforcement*.** The FCC also levied fines against companies for lax data security standards. In July 2023, the FCC sought a combined $20 million fine against two mobile carriers for alleged violations of FCC rules, which mandate that customer identity be properly authenticated before online access to Customer Proprietary Network Information (“CPNI”) is granted to them.[302] The FCC’s investigation concluded that the companies used “readily available” information to provide online access to CPNI and fell below other compulsory data security standards in violation of multiple parts of the FCC’s rules, thereby placing sensitive customer personal data at risk.[303] **6. State Agencies** Throughout 2023, state privacy enforcers, particularly in California, wielded their authority to attempt to expand the ambit of existing privacy laws. **a. California** California Privacy Protection Agency On the rulemaking front, the California Privacy Protection Agency (“CPPA”) released draft rules for automated decision-making technology (“ADMT”) on November 27, 2023.[304] The draft focuses on two areas: notice requirements on the use of ADMT and enforcement of two new consumer rights: the right to opt-out of ADMT processing and the right to access information about a business’s use of ADMT. The draft rules require businesses to provide a “Pre-use Notice” which would allow consumers to exercise these two rights. The notice must inform consumers of the business’s use of ADMT and permit them to opt-out of ADMT processing. It also requires businesses to describe the purpose behind the use of ADMT in specific terms. Consumers may opt-out of ADMT for decisions that produce “legal or similarly significant effects” (1) as an employee, student, job applicant or independent contractor or (2) in publicly accessible places (e.g., via surveillance or facial recognition). Formal rulemaking is expected to begin in early 2024. The CPPA has also begun to spin up its enforcement division, which began inquiring into manufacturers of connected vehicles, meaning vehicles embedded with features like location sharing, web-based entertainment, smartphone integration, and cameras, in an effort to better understand whether companies in this space are complying with applicable rules.[305] California Attorney General The California Attorney General (“CA AG”) has announced several privacy-related enforcement “sweeps” in 2023 in a variety of industries. In early 2023, the CA AG sent out letters to an unspecified number of mobile apps in the retail, travel, and food service industries that purportedly failed to comply with the CCPA, specifically by failing to honor consumer requests to opt out of the sale of their personal data or providing mechanisms for opting out of sale of the personal data.[306] In July 2023, the CA AG announced a separate sweep of large employers’ compliance with CCPA as it related to employee and job applicant information.[307] Businesses are required to provide a way for consumers, workers, and job applicants to be able to access, delete, and opt-out of the sale of their personal information. Despite these regular sweeps, however, the CA AG has not announced any enforcement actions or settlements related to the CCPA. Although there have not been any CCPA settlements disclosed in 2023, the CA AG did announce a $93 million settlement with a large technology company related to allegations that its location-privacy practices violated California’s Unfair Competition Law, a follow-on to a multistate settlement announced in 2022.[308] The complaint alleged that the company deceived people into consenting to the perpetual collection and use of their location data by asking users if they wanted to “enhance” their “experience.” The complaint also alleged that, even if users turned off their location history, their precise location data was nevertheless collected if other settings remained enabled. Finally, the CA AG alleged that the company continued to use real-time location information to show users ads, even if they turned off ad personalization. Under the terms of the settlement, the company will have to provide a pop-up notification to users who have certain location-tracking toggles enabled, provide additional disclosures to users (including in the account-creation flow) and obtain express

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

affirmative consent prior to sharing precise location information with advertisers, among other requirements. The company will also have to submit an annual compliance report and independent assessor reports. **b. Other State Agencies** New York In January 2023, the New York Attorney General ("NY AG") sent a letter to a large live-entertainment company about its use of facial recognition technology that allegedly was preventing entry into its venue by attorneys whose firms are engaged in litigation against the company.[309] The NY AG's letter requests the company provide justifications for its policy, identify efforts to comply with applicable laws, and ensure that its use of this technology will not lead to discrimination. In November 2023, the New York State Department of Financial Services announced that a title insurer will pay $1 million for allegedly violating state cybersecurity regulations.[310] The insurer allegedly failed to ensure "full and complete implementation" of its cybersecurity policies and procedures prior to a May 2019 data breach that exposed its customers' nonpublic information.[311] Washington The Washington Attorney General ("WA AG") announced a $39.9 million settlement with a large technology company related to the WA AG's lawsuit over its location-tracking practices.[312] The WA AG, like the CA AG, filed a separate lawsuit from the multistate effort that had been settled in November 2022. Similar to the California suit, the WA AG alleged that the company collects location data even when consumers had disabled their location history and that it tracked devices even when location access was turned off. In addition to the monetary penalty, the company agreed to disclose additional information to users where they enabled location-related account setting, ensured that users see information about location tracking and gave users detailed information about types of location data that the company collects and how it will be used. **c. Major Data Breach Settlements** While 2023 did not see as many high-profile data breach settlements as in recent years, with the number of data breach-related case filings reaching new records, major settlements are likely on the horizon. Many of the notable 2023 settlements were reached with state attorneys general. A software provider in the healthcare and education space agreed to a $49.5 million settlement with numerous state attorneys general (led by Indiana and Vermont) to resolve claims stemming from a ransomware attack that impacted the company and nearly 13,000 customers in 2020.[313] In another notable data breach settlement, the attorneys general of New York, Connecticut, Florida, Indiana, New Jersey, and Vermont entered into a $6.5 million settlement with a major financial services provider arising from two instances in which customer data inadvertently left the company's custody.[314] And a vision insurance company entered a $2.5 million settlement with the attorneys general of New Jersey, Oregon, Florida, and Pennsylvania stemming from a breach which impacted the health care information of 2.1 million individuals.[315] Class actions have also resulted in significant settlements. A law firm recently announced that it reached a tentative class settlement with plaintiffs whose personal information was allegedly compromised in a data breach.[316] Once finalized, this settlement will resolve four consolidated lawsuits stemming from the firm's alleged three-month delay in notifying affected individuals of the breach. And in July 2023, the Southern District of Florida approved a $3 million settlement in a class action suit against a health care network and its parent company arising from a 2021 data breach in which over three million individuals were affected.[317] **III. Civil Litigation Regarding Privacy and Data Security A. Data Breach Litigation** Cybercrimes targeting consumer data have been increasingly pervasive and this trend continued in 2023. The Identity Theft Resource Center, which compiles statistical information on data breaches, reported 2,116 data breaches in the first nine months of 2023.[318] This number surpasses the 2021 record of 1,862 data breaches and represents a nearly 64% increase of the number of data breaches reported over the same nine-month period in 2022.[319] These trends suggest companies will continue to face more widespread and sophisticated attacks by cybercriminals and the risk of litigation remains elevated for companies dealing with the aftermath of a cyberattack. One of the largest and most significant data breach litigations in history was filed this year. After the developer of a popular file transfer service announced that its service had been exploited by a Russian cybergang in a data breach that exposed the personally identifiable information of more than 55 million people, more than 200 cases were filed.[320] These actions were centralized in an MDL that is now pending in the District of Massachusetts.[321] At the time of publication, the MDL remains in its early stages, but we expect this case will be one that practitioners will watch closely.

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

This section summarizes key developments in data breach litigation last year. **1. The Impact of *TransUnion v. Ramirez* on Standing in Data Breach Actions** Many data breach cases are litigated in federal court, given large numbers of potentially affected individuals and jurisdictional provisions of the Class Action Fairness Act. Plaintiffs pursuing claims in federal court must satisfy the standing requirements of Article III of the U.S. Constitution, and data breach actions raise significant questions about whether plaintiffs can satisfy this requirement. In 2021, the U.S. Supreme Court decided *TransUnion v. Ramirez*, a landmark decision that increased the burden on plaintiffs to demonstrate standing in actions for money damages brought in federal court.[322] The Court held that the mere risk of future harm is insufficient to satisfy the concrete injury that Article III requires, especially where the plaintiff is unaware of the risk of future harm.[323] This holding is especially significant in data breach cases where a plaintiff's data has been breached but not yet misused. Although *TransUnion* went a long way towards clarifying how risks of future harm should be analyzed under Article III, appellate courts have continued to grapple with the bounds of the Court's holding and divergent approaches to the issue of standing persisted in 2023. Some courts have interpreted *TransUnion* narrowly and concluded that notwithstanding its holding, plaintiffs can establish standing even if their data has not yet been misused. For example, in *Webb v. Injured Workers Pharmacy, LLC*, the First Circuit held that a "material risk of future harm can satisfy the concrete-harm requirement" for standing, reasoning that data compromised in targeted attacks (as opposed to inadvertent disclosures) is more likely to be misused, especially when the data is sensitive and other personal information in the exposed data has already been misused.[324] Moreover, to satisfy *TransUnion*'s requirement of "alleg[ing] a separate, concrete present harm" to have standing to seek damages, the court held that the plaintiffs' "time spent responding to a data breach can constitute a concrete injury sufficient to confer standing, at least when that time would otherwise have been put to profitable use."[325] Similarly, the Second Circuit held that a plaintiff suffered "concrete harms as a result of the risk of future harm occasioned by the exposure" of her personal information, in particular because she incurred expenses attempting to mitigate the consequences of the breach.[326] Moreover, the plaintiff's name and Social Security number were compromised in the targeted attack, and the court reasoned that the exposure of this type of sensitive data led to concrete present harms due to the increased risk that her identity would be stolen in the future.[327] Other courts have interpreted *TransUnion* to mandate a stricter approach to standing. For example, in *Holmes v. Elephant Insurance Co.*, a trial court dismissed for lack of standing claims alleging that the plaintiffs' personal information was compromised in a 2022 data breach.[328] Despite a potential heightened risk of future identity theft, the court found that this risk alone did not constitute an injury in fact unless it was "certainly impending."[329] Even though two of the three named plaintiffs had alleged their driver's license information had appeared on the dark web, the court reasoned that unless combined with additional personal information, a driver's license number could not be used to create a full identity profile, and therefore only constituted a threat of future identity theft.[330] The court also found there was insufficient support for the contention that the risk of identity theft was "certainly impending" without assuming that the plaintiffs were specifically targeted in the breach, that the perpetrator was actively compiling full profiles of plaintiffs, and that the perpetrator would "imminently and successfully attempt to use th[e] information [at issue] to steal the plaintiffs' identities."[331] In reaching this conclusion, the court also diverged from the approach taken by the First Circuit in *Webb*, finding that absent an imminent threat of identity theft, the cost of mitigative measures, such as time spent monitoring financial information, does not constitute an injury sufficient to support standing.[332] A California district court in *Burns v. Mammoth Media, Inc.*, appeared to agree with this approach, suggesting that "an increased risk of identity theft may constitute a credible threat of real and immediate harm sufficient to constitute an injury in fact for standing purposes."[333] However, the court ultimately denied standing and dismissed the claims because there were insufficient allegations to establish an increased threat of identity theft based on the type of data compromised. In particular, the plaintiff alleged only that his name, email address, gender, profile creation date, user name, user ID, password, and access token were exposed, but he failed to explain how the specific data compromised was sufficiently sensitive to create a risk of identity

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

theft.[334] Questions about standing are also significant to class certification, as putative classes that contain large numbers of uninjured class members are frequently not viable.[335] One case from 2023 illustrating this issue is *Attias v. CareFirst, Inc.*, where the District Court for the District of Columbia denied class certification because "the proposed classes . . . would appear to sweep in significant numbers of people who have suffered no injury in fact in light of *TransUnion*."[336] Even though the named plaintiffs had adequately demonstrated standing "because they ha[d] spent at least some amount of time or money protecting against the risk of future identity theft," there was a "serious predominance problem" because not all the putative class members had done the same, thereby necessitating "individualized proof of injury."[337] These "logistical hurdles of identifying class members who were injured or determining what kinds of mitigation measures might qualify an individual for class membership" meant the court "[could not] conclude that the common issues predominate over individualized inquiries."[338] **2. Cybersecurity-Related Securities Litigation** In the aftermath of a cybersecurity incident, companies and their officers also frequently face shareholders suits. Although the pace of data breach-related securities case filings has slowed,[339] the past year still saw a fair share of new litigation. For instance, in March 2023, shareholders filed a securities class action under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 against a television service provider, alleging that the company overstated its operational efficiency in public statements and SEC filings and maintained deficient cybersecurity infrastructure, leaving the company unable to secure customer data and leaving it vulnerable to cyberattacks and service issues.[340] In another action filed in 2023, shareholders alleged that a financial services technology company violated Sections 12(a)(2) and 15 of the Securities Act of 1933 in connection with the compromise of customer data.[341] The plaintiffs alleged that the company failed to accurately describe its data security capabilities, among other things, in its securities filings. This case remains in the early stages. Defendants have had success in getting shareholder data-breach claims dismissed on the pleadings, including for failure to plead falsity or scienter with the requisite particularity.[342] For example, the Northern District of California dismissed a shareholder suit related to a January 2022 data security incident.[343] The plaintiffs in that case sued under Section 10(b) and 20(a) of the Securities Exchange Act of 1934, alleging that the company and certain officers made false and misleading statements in the company's disclosures about its data security practices.[344] The court dismissed these allegations, finding that the plaintiffs failed to allege either falsity or scienter based on the defendants' general statements about the company's commitment to data security.[345] **B. Wiretapping and Related Litigation Concerning Online "Tracking" Technologies** Last year's Review noted a deluge of lawsuits brought under federal and state wiretapping statutes. This trend continued in 2023, with recent lawsuits alleging that various businesses invade consumers' privacy rights and violate federal and state wiretapping statutes by allegedly failing to obtain sufficient and valid consent when using various online "tracking" technologies, such as session replay, pixels, and chat software. Plaintiffs in these cases generally allege that their interactions with businesses' websites or apps are "communications" between them and the business, which are being "recorded" and "intercepted" by the business through a third-party pixel, software development kit, chat, or session-replay service provider.[346] Many of these cases focus on claims for violations of wiretapping statutes. Wiretapping statutes were initially intended to prevent surreptitious recording of, or eavesdropping on, phone calls without the consent of the parties involved, but they have evolved to cover other forms of electronic and digital communications. The federal Wiretap Act of 1968, as amended by the Electronic Communications Privacy Act of 1986,[347] is a "one-party" consent statute that allows communications to be intercepted (with certain exceptions) so long as "one of the parties to the communication has given prior consent[.]"[348] Almost all 50 states also have some form of wiretapping statute; most of them are also one-party consent statutes, but a significant minority require "two-party" (or "all-party") consent.[349] Many recent lawsuits have brought claims under both the federal Wiretap Act and various state statutes, with litigation heavy in all-party consent states like California (where statutory damages can run as high as $5,000 per violation), Pennsylvania, and Florida.[350] In addition to alleged violations of wiretapping statutes, lawsuits concerning online tracking technologies frequently raise a host of interrelated legal issues. For example, a plaintiff in a Northern District of California case alleged that a

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

pixel tool was embedded in a university-owned hospital website where the plaintiff entered private medical information concerning her cardiovascular health.[351] Because this information was allegedly redirected to a third-party company, the plaintiff claimed that the defendant violated the California Invasion of Privacy Act ("CIPA"), three separate sections of the Confidentiality of Medical Information Act ("CMIA"), and the California Constitution. The plaintiff also alleged common law causes of action including breach of contract, unjust enrichment, and the right to privacy. The court allowed the common law privacy and two CMIA claims to move forward and dismissed the remaining claims, largely on the basis that the university is an immune public entity. Similarly, in *Jackson v. Fandom Inc.*,[352] another Northern District of California judge denied the defendant's motion to dismiss a proposed class action alleging that the defendant, a hosting service for user-generated wikis, violated the federal Video Privacy Protection Act ("VPPA") by sharing users' personally identifiable information ("PII") through pixels. Specifically, the judge found that associating viewing history with the plaintiff's unique user ID may have constituted unlawful disclosure of PII.[353] In yet another notable decision, a federal judge dismissed claims against a technology company alleging it had shared information about the plaintiffs' online activity with a third party via a pixel without the plaintiffs' consent.[354] The plaintiffs claimed that the company's terms of use did not inform users that the platform was sharing information with the third party and that its failure to disclose this information was fraud by omission in violation of both California's Unfair Competition Law ("UCL") and its Consumer Legal Remedies Act ("CLRA"). They also asserted claims under VPPA and for unjust enrichment. In granting the company's motion to dismiss these claims, the court reasoned that Rule 9(b)'s heightened pleading standard applied because the alleged fraud stemmed from alleged misrepresentations in the company's terms of use.[355] The court therefore granted the company's motion to dismiss the CLRA and UCL claims. In November 2023, the company moved for summary judgment on that claim, which remains pending. These cases are representative of many others, and we expect plaintiffs to leverage their mixed outcomes to continue to bring and attempt to extract settlements in similar matters. **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."[356] In recent years, several high-profile court decisions, including the U.S. Supreme Court's 2021 decision in *Van Buren v. United States*, have limited the CFAA's scope.[357] In 2022, these decisions also prompted the Department of Justice to narrow its CFAA enforcement policies,[358] as described in last year's Review. **1. CFAA** In 2023, courts around the country have continued to grapple with the CFAA's outer bounds. Summarized below are three cases of particular interest, including a case from the Second Circuit analyzing venue considerations in CFAA actions and a pair of district court cases reaching somewhat different conclusions on whether software constitutes a "computer" under the statute. ***Venue in CFAA Criminal Cases.*** In July 2023, the Second Circuit upheld a criminal CFAA conviction against a venue challenge.[359] The case involved a defendant, a disgruntled former employee, who deleted information from her company's online database, which was hosted on servers outside of New York.[360] Her deletion of the database prevented some employees in New York from accessing it.[361] A criminal action was brought against the defendant in the Southern District of New York and the defendant argued venue was improper because the data she deleted resided on servers in Virginia and California, and therefore she could not have damaged a computer in New York.[362] The Second Circuit rejected this claim, holding that even though the data was stored on cloud servers elsewhere, the defendant had still "damaged" a computer in New York, because she had "impair[ed] . . . the integrity or availability of data, a program, a system, or information" on a computer there.[363] The Supreme Court denied certiorari.[364] The case is notable not just because of its expansive view of venue in CFAA criminal cases, but also because it raises new questions about the scope of covered harm to "protected computers" in CFAA criminal and civil cases alike—an especially important issue given the interconnectedness of computer networks. ***Cloud Computing Systems As Covered "Computers."*** In July 2023, an Illinois federal district court held that a "cloud-based system of data storage" constitutes a "computer" under the civil enforcement sections of the CFAA.[365] The defendants in this case allegedly accessed a former employer's Microsoft Office 365 cloud services after their employer

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

terminated them—by logging in with old and phony credentials.[366] The defendants moved to dismiss the employer's CFAA claim, arguing a cloud service is not a protected "computer" under the CFAA.[367] The court disagreed.[368] The court reasoned that the CFAA broadly defines a "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."[369] Because a cloud system involves storing data on remote servers, and "[s]ervers fit within the plain language" of a computer under the Act, the plaintiff had sufficiently alleged that the defendants improperly accessed a "computer" under the CFAA.[370] The court also rejected the premise that CFAA liability could attach only if the *plaintiff*, rather than Microsoft, actually owned the remote servers that supported the cloud service.[371] ***Software Not a Covered "Computer."*** By contrast, in April 2023, a New Jersey federal district court held that "software" does not constitute a protected computer under the CFAA.[372] In this case, the plaintiff claimed that he was hired to install certain software he created on a bank's computers, but a dispute arose over whether the bank had paid for a license to use the software.[373] The plaintiff sued, claiming, among other things, that by using the software without permission and by locking him out of his bank computer (which allegedly contained the software), the bank violated the CFAA.[374] The court summarily disagreed, noting that the plaintiff had presented "no authority indicating that software is a 'computer' within the meaning of the CFAA," and dismissed the claim.[375] ***Generative AI and the CFAA.*** Another notable development from this past year was the bevy of lawsuits filed against generative AI companies, challenging the companies' alleged practice of scraping or otherwise obtaining data to train their AI models. Some of these lawsuits claim that these practices—which involve allegedly harvesting publicly accessible data from the Internet or obtaining user data through the use of "plug-ins" installed on third-party websites—violate the CFAA for exceeding authorized access to plaintiffs' computers.[376] These cases are still at their early stages and will likely need to grapple with the Ninth Circuit's 2022 decision in *hiQ Labs, Inc. v. LinkedIn*,[377] which held that the CFAA's concept of "without authorization" may not apply "when a computer network generally permits public access to its data"—although the Ninth Circuit noted there may be other common law and statutory claims available for those who believe they have been the victims of data scraping.[378] **2. CDAFA** The Comprehensive Data Access and Fraud Act ("CDAFA") is California's sister statute to the CFAA, and it creates a private right of action against any person who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network."[379] "Access" means to "cause output from" the "logical, arithmetical, or memory function resources of a computer."[380] In 2023, several district courts considered the interaction between the CDAFA and the recent wave of litigation related to website tracking technologies, including web pixels. Below are two such cases of interest. ***Private Browsing Modes and Online Advertising Technologies.*** In August 2023, a California district court denied a motion for summary judgment on a CDAFA claim. Plaintiffs alleged that a prominent internet company improperly tracked user activity when users were using "private browsing modes."[381] Plaintiffs claimed that, when third parties embedded certain advertising technologies into their websites, those technologies sent data about the users' online activities to the company, even if the users were using a private browsing mode.[382] The company sought summary judgment on plaintiffs' CDAFA claim, arguing that the company could not have "accessed" plaintiffs' computers under the CDAFA because "website developers," not the defendant, embed the code that directs users' browsers to send requests to the company's servers."[383] The court rejected this argument, holding that the fact that "website developers chose to embed [the company's] services onto their websites at most creates a triable issue as to whether developers and not the company . . . 'cause output from' plaintiffs' computers" under the CDAFA.[384] The company separately argued that plaintiffs had suffered no "damage or loss" under the CDAFA, but the court rejected this argument, too, holding that "plaintiffs [had] proffer[ed] evidence that there is a market" for their browsing history data.[385] On December 26, 2023, the parties announced that they had reached a preliminary settlement agreement.[386] ***"Technical Barriers" for First-Party***

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Websites. In October 2023, a California district court dismissed with prejudice a CDAFA claim premised on the theory that a chatbox on a developer's website transmitted certain user information to third parties.[387] The developer argued that it did not act "without permission" under the CDAFA because it did not overcome any "technical or code-based barriers" to insert the third-party code into its own website and allegedly transmit user information.[388] The district court agreed, holding that there are "no technical barriers blocking Defendant from using its own Website" in the manner alleged.[389] The district court also dismissed the claim on the basis that plaintiff had failed to allege any damage or loss under the CDAFA.[390] **D. Telephone Consumer Protection Act Litigation** Originally enacted in 1991, the Telephone Consumer Protection Act ("TCPA") regulates certain forms of telemarketing and the use of automatic telephone dialing systems ("ATDS").[391] Historically, much of TCPA litigation centered on issues concerning the technical definition of an ATDS, but that issue was largely clarified through the Supreme Court's 2021 opinion in *Facebook Inc. v. Duguid*, which favored a narrower definition that limited it to devices that store or produce telephone numbers by using a random or sequential number generator. [392] Nonetheless, the TCPA continues to be an area of significant regulatory and litigation activity. 2023 was defined by increased regulation and enforcement by the FCC, as well as ongoing federal litigation addressing the scope of the TCPA. TCPA cases continue to make their way up to the federal appellate courts, which frequently present the issue of whether receipt of a single unsolicited call is sufficient to confer Article III standing. Some circuits have answered in the affirmative. For example, the Sixth Circuit held that a consumer who had received a ringless voicemail had standing to sue under the TCPA.[393] The plaintiff argued, successfully, that the receipt of the unsolicited ringless voicemail was comparable to the common law tort of intrusion upon seclusion.[394] Similarly, in *Drazen v. Pinto*, an en banc panel of the Eleventh Circuit held that individuals who received even a single unwanted telemarketing text message had standing to sue under the TCPA, overruling the court's prior decision that held the opposite.[395] In another notable decision, *Hall v. Smosh Dot Com, Inc.*, the Ninth Circuit held that a phone line subscriber has standing to sue for TCPA violations, even if the subscriber is not the recipient of the call.[396] Even though the plaintiff's son in that case had received the unwanted text messages, the Ninth Circuit stated that the TCPA does not require that "the owner of a cell phone must also be the phone's primary or customary user to be injured by unsolicited phone calls or text messages sent to its number."[397] Not all courts have read the TCPA so expansively, and appellate courts continue to find communications not covered by the language of the TCPA. For example, in January 2023, the Third Circuit held that faxes sent by a drug testing laboratory, promoting a free educational seminar about opioid use and medication monitoring, did not qualify as "unsolicited advertisements" under the TCPA.[398] In another notable case, the Ninth Circuit held that text messages did not violate the TCPA's prohibition on "prerecorded voices," because text messages are not "voice" messages.[399] In the face of newly implemented rules, shifting case law, and new communications technology, we expect the TCPA to continue to be an area to watch. **E. State Law Litigation 1. California Consumer Privacy Act Litigation** While the regulatory atmosphere around the CCPA evolved in 2023, the litigation landscape remained fairly constant. Consumers, individually or as a class, continued to litigate under the CCPA, making claims for both pecuniary and statutory damages. **a. Potential Anchoring Effect of CCPA Statutory Damages** As discussed in last year's Review, the CCPA's provisions for statutory damages have continued to frame settlement negotiations. The CCPA provides that consumers exercising their private right of action for a data breach may recover the greater of statutory damages between $100 and $750 per consumer, per incident, or actual damages.[400] The cases summarized below provide color on how these statutory damages have impacted settlement terms in the CCPA context. ***Automobile Manufacturers and Marketing Vendor.*** In this case, previously discussed in last year's Review, residents of California and Florida filed class actions alleging that auto manufacturers and a marketing vendor failed to adequately secure customers' personal information, allowing hackers to steal information such as driver's license numbers, Social Security numbers, financial account numbers and more.[401] The plaintiffs asserted causes of action for negligence, breach of implied contract, violation of the CCPA, violation of California's Unfair Competition Law, and breach of contract. The parties agreed to a

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

settlement which was granted final approval on May 31, 2023.[402] The terms of the settlement reflect the potential effects of the CCPA, as California residents whose sensitive personal information was affected received $350, while the non-California residents whose sensitive personal information was exposed would receive only $80 (about 77% less than their California peers).[403] ***Ticket Retailer*.** Consumers who bought tickets from a ticket retailer brought suit after a data breach was disclosed. Plaintiffs alleged that "skimmers" placed on the defendant's checkout webpage stole their personal sensitive data.[404] Plaintiffs asserted a variety of claims, including negligence, breach of contract, violation of California's Unfair Competition Law, and violation of the CPPA.[405] The parties reached a $3 million settlement, which was granted final approval on October 30, 2023. The settlement fund provides California sub-class members with an additional $100 "California Statutory Award benefit."[406] **b. Requirements for Adequately Stating a CCPA Claim** Courts continued to give shape to the requirements to plead a CCPA claim. The decisions below address the facts and allegations required to bring a CCPA action under its limited private right of action, which applies only to data breaches. ***Software Company Automatic Renewal Case*.** The Ninth Circuit recently affirmed the dismissal of a case alleging violations of the CCPA. The plaintiff alleged his data was shared with a credit card processor without his authorization due to the automatic renewal of his subscription. The trial court dismissed his claim because the plaintiff had agreed to the defendant's End-User License Agreement, which stated his subscription would renew every 12 months unless terminated.[407] The trial court found the disclosure of his personal information was not "without authorization" and was not caused by a failure to implement reasonable security procedures and practices.[408] The Ninth Circuit affirmed.[409] ***Online Banking*.** Plaintiff alleged that the defendant bank violated the CCPA when an unknown individual accessed his bank account, changed his contact information, and obtained new account cards to make purchases. The bank, on a motion to dismiss, argued that the plaintiff had not alleged that a data breach occurred. The court disagreed, finding that plaintiff's allegations that his account was accessed and personal information obtained because of the failure to implement reasonable security procedures were sufficient to state a claim under the CCPA.[410] **c. CCPA Violations Under the UCL** Violations of the CCPA cannot serve as the predicate for a cause of action under a separate statute including California's Unfair Competition Law ("UCL").[411] While there has been no change regarding the inability to use a CCPA violation as the predicate "unlawful" claim under the UCL, one court has found the CCPA may create a property interest upon which a UCL claim may be brought. That decision is summarized below. ***Search Engine Company*.** Originally filed in June 2020, this class action alleges that a large technology company unlawfully collected data from users while using the company's browser in incognito or private mode.[412] The plaintiffs brought claims, including under the federal Wiretap Act, the California Invasion of Privacy Act (CIPA), and California's UCL.[413] On summary judgment, the defendant argued that plaintiffs had no economic injury as required for a UCL claim, as they had not lost money or property as a result of the data collection.[414] Plaintiffs argued that their private data has monetary value and they have a property interest in that data "because the [CCPA] affords them the right to exclude Google from selling their data to third parties."[415] The court agreed with plaintiffs, holding that "plaintiffs have identified an unopposed property interest for at least a portion of the class period under the California Consumer Privacy Act."[416] The court further found that money damages are not an adequate remedy alone, and that injunctive relief is necessary to address the ongoing data collection.[417] **d. The CCPA's 30-Day Notice Requirement** The CCPA requires that a "consumer provide[] a business 30 days' written notice identifying the specific provisions of [the CCPA] the consumer alleges have been or are being violated."[418] The written notice initiates a 30-day period during which the business may cure any violation. While this cure provision was eliminated by the CPRA, cases addressing the notice-and-cure provisions have continued to move through the courts. Last year's Review discussed a case dismissing a suit with prejudice where plaintiffs did not comply with the 30-day notice period.[419] The cases below have departed from that decision, illustrating the boundaries of the cure provision as a safeguard. ***Consumer Debt Collector*.** Plaintiffs alleged that their personal information was stolen in a data breach because the information was unencrypted and improperly safeguarded.[420] Plaintiffs brought claims under the CCPA for actual and statutory

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

damages, even though they provided no pre-suit notice for the defendant to cure as required under the CCPA.[421] The court noted that no pre-suit notice is required to the extent plaintiffs sought pecuniary damages, but dismissed the statutory damages claims without prejudice.[422] In dismissing the claim for statutory damages without prejudice, the court expressly declined to follow *Griffey*, which we discussed in last year's Review. The *Griffey* court had dismissed a CCPA claim with prejudice, reasoning that the purpose of the pre-suit notice is to allow the defendant time to cure the violation out of court.[423] Allowing a plaintiff to file a complaint, then send a notice, and then file an amended complaint defeats this remedial purpose of the statutory notice-and-cure provision. The Western District of Washington expressly rejected *Griffey*'s rationale, concluding that dismissal without prejudice "accords with the remedial nature of the CCPA's notice provision."[424] ***Money Services Business*.** After a data breach, plaintiffs brought suit claiming negligence, breach of implied contract, and violation of the CCPA due to the disclosure of their names, Social Security numbers, and driver's license numbers.[425] Defendant moved to dismiss the CCPA claim, arguing it was barred due to the notice-and-cure provision. Defendant "claimed to have enhanced its security measures" after receiving notice of the alleged violation, and thus "cured all alleged violations within the requisite time period."[426] The court found this straightforward assertion insufficient because "the implementation and maintenance of reasonable security procedures and practices . . . following a breach does not constitute a cure with respect to that breach."[427] The court pointed out that the defendant had not provided any additional detail on the nature of its cure, concluding that this was insufficient at the motion-to-dismiss stage.[428] **e. Guidance on Reasonable Security Measures in Connection with the CCPA** In addition to the cases highlighted by last year's Review,[429] courts have continued to weigh in on what qualifies as reasonable data security measures under the CCPA. ***Moving Company*.** Plaintiffs brought suit after their personal information was stolen by hackers in a cyberattack. Plaintiffs asserted violations of the CCPA for failure to take reasonable precautions to protect their personal information.[430] The court declined to dismiss the CCPA claim, and identified a number of measures the defendants could have taken prior to the breach. Plaintiffs specifically alleged that the defendant's security measures were inadequate because they failed to implement "adequate filtering software," "adequate[] training," "multi-factor authentication," encryption, and destruction when the personal information was no longer in use.[431] The court also pointed to plaintiff's complaint, which "identif[ied] fourteen cybersecurity best practices that defendant should have followed but allegedly did not."[432] ***Large National Bank*.** Plaintiffs brought numerous claims arising out of prepaid benefits payment cards issued by the bank.[433] Plaintiffs alleged that these cards were targeted by bad actors, and the information was easily accessible since the cards had magnetic strips instead of chips. Plaintiffs claimed that erroneous charges and unauthorized transactions resulted in the loss of their funds and alleged violations of the CCPA due to the debit cards' lack of chip technology, asserting that use of chip technology is a necessary reasonable security measure to protect their personal information. The court agreed, finding that the allegations stated a claim under the CCPA.[434] The court also found that plaintiffs' allegation that the bank failed to subject its agents to background checks was adequate to state a claim based on failure to implement and maintain reasonable security measures and practices.[435] **2. State Biometric Information Litigation a. Illinois Biometric Information Privacy Act** 2023 was another active year for Illinois's biometrics law, with courts continuing to expand the scope of the Biometric Information Privacy Act ("BIPA"), but also recognizing new limitations. Perhaps unsurprisingly, Illinois also continued as the leading state with respect to biometrics-related litigation. **i. Expansion of BIPA's Scope** ***BIPA's Statute of Limitations Under Section 15.*** The Supreme Court of Illinois found that claims brought under Section 15 of BIPA (which relates to retention, collection, disclosure, storage, and use of biometric information) have a five-year statute of limitations, reversing an appellate court's ruling that placed a one-year limit on such claims.[436] Under Illinois law, "actions . . . to recover damages for an injury done to property, real or personal . . . and all civil actions not otherwise provided for, shall be commenced within 5 years next after the cause of action accrued."[437] Part of the court's justification for finding that the default Illinois statute of limitations five-year catchall applied was because a shorter limit would "thwart [the] legislative intent" of BIPA to provide

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

redress for persons aggrieved and "shorten the amount of time a private entity would be held liable for noncompliance with the Act."[438] Additionally, upon a certified question from the Seventh Circuit, the Supreme Court of Illinois ruled in a 4-3 decision that BIPA claims "accrue under the Act each time a private entity scans or transmits an individual's biometric identifier or information in violation of section 15(b) or 15(d)."[439] The court dismissed ongoing policy-based concerns about massive damages by reiterating that the court "has repeatedly recognized the potential for significant damages awards under the Act" and that such high damages operate as an incentive for private entities to conform to state law.[440] While noting trial courts presiding over a class action "possess the discretion to fashion" a fair yet less-deleterious award, the court concluded that the legislature was the best vehicle to address policy concerns and the plain language of the statute authorized accrual of claims.[441] ***BIPA Claims Survive Death.*** Also in 2023, a federal court in Illinois, hearing a class action case where the named plaintiff passed away, held that BIPA created a personal property interest and claims survive the plaintiff's death.[442] **ii. New Recognized Limitations Under BIPA** Even so, courts recognized limitations to claims brought under BIPA in 2023. ***"Active Steps" In Furtherance of Collecting Biometric Data*.** For example, an Illinois federal judge dismissed two claims in a proposed class action where an employer used third-party timekeeping software that registered and scanned employee fingerprints which were then stored on a vendor's cloud storage service.[443] The judge held that the cloud storage vendor did not take an "active step" in furtherance of collecting biometric information merely by contracting with the third party to provide access to the vendor's cloud storage system, but instead was "merely a vendor to the third party that provided the biometric timekeeping technology and services to [the employer]."[444] ***Exceptions to Collections of Biometric Data:*** In some cases, courts found that certain exceptions privileged the collection of biometric data—for example, one trial court held that the "general health care exemption" to BIPA covered a virtual try-on tool for sunglasses, finding sunglasses to be a Class I medical device under the FDA.[445] Another court denied the plaintiff's motion to strike the defendant's affirmative defense that "the biometric identifiers it collects fall within [the general health care] exception because they are collected along with medical information provided by a donor," such as fingerprints taken prior to donating plasma used to identify the patient during each donation.[446] The court noted that BIPA does not define the term "patient" nor does it define the term "health care" and found that the defendant's arguments as to why the exception applied were sufficient to survive a motion to strike.[447] **b. Texas Biometric Privacy Law Litigation** As discussed in last year's Review, in February 2022, Texas Attorney General Ken Paxton brought the first enforcement action under the Texas Capture and Use of Biometric Identifier Act ("CUBI") more than two decades after its passage in 2001.[448] AG Paxton asserted a CUBI claim against a large social media company alleging that the company's collection of "facial geometries" in connection with its facial recognition and tagging feature that it deprecated in November 2021 violated CUBI, in addition to bringing claims under Texas' Deceptive Trade Practices Act.[449] The parties continued to conduct discovery in the case throughout 2023. In late October 2022, Texas filed a similar action against another large technology company for alleged violations of CUBI.[450] The case is still in the early stages of discovery. These two cases remain the only actions brought under CUBI. Given the preliminary enforcement efforts by the state of Texas, companies can continue to expect heightened state-level scrutiny and enforcement in the biometrics arena in 2024. **c. New York Biometric Privacy Law Litigation** 2023 also saw challenges under the N.Y.C. Biometric Privacy Law. On May 19, 2023, two plaintiffs filed a class action against a large live-entertainment company for its alleged use of facial recognition software to keep banned individuals out of its venues.[451] The plaintiffs allege that the company collects biometric information from every person who enters its venues, and then compares that information to an internal database of banned individuals.[452] The complaint further alleges that the company shares this biometric information with at least one third-party vendor, and that the company ultimately benefits in the form of reduced litigation costs.[453] The plaintiffs allege that this undisclosed collection, use, and disclosure of customers' biometric data violates the 2021 New York City Biometric Identifier Information Law and the right to privacy guaranteed by Article 5 of the New York Civil Rights Law.[454] Plaintiffs also pleaded an unjust enrichment claim, maintaining that the company wrongfully obtained

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

benefits from the proposed plaintiff class in the form of valuable data.[455] On January 9, 2024, a federal magistrate judge released a report recommending dismissal of the civil rights and unjust enrichment claims.[456] On the civil rights law claim, the court found that the limitations period of one year had already run for one plaintiff.[457] For the other plaintiff, the court found that the defendant's alleged collection and use of biometric information to remove banned individuals could not plausibly be understood "as seeking to draw trade at its venues"—a necessary element of a claim under the civil rights statute.[458] The magistrate also recommended dismissing the unjust enrichment claim on the ground that "New York courts have long recognized the Civil Rights Law as 'preempting all common law claims based on unauthorized use of name, image, or personality, including unjust enrichment claims.'"[459] Thus, under New York law, there can be no unjust enrichment claim arising from use of one's personal image.[460] The magistrate recommended allowing the New York City Biometric Identifier Law claim to proceed, finding that the defendant's alleged conduct is consistent with the text and legislative history of the statute.[461] **F. Other Noteworthy Litigation** ***Supreme Court Declines to Address Scope of Section 230.*** In last year's Review, we noted that the U.S. Supreme Court granted certiorari in two cases that could affect the scope of Section 230 of the Communications Decency Act of 1996, which protects "interactive computer services" from liability for user-published content. In each case, *Twitter, Inc. v. Taamneh*[462] and *Gonzalez v. Google LLC*,[463] plaintiffs alleged that social media companies were liable under the Anti-Terrorism Act (ATA) for aiding and abetting acts of terrorism that resulted in the deaths of plaintiffs' family members. According to the plaintiffs, ISIS allegedly used the defendants' websites to fundraise and recruit new members, with little interference by content moderators—and sometimes even active promotion by the defendants' algorithms. Both cases came from the Ninth Circuit Court of Appeals, which had allowed the *Taamneh* case to proceed[464] but held that Section 230 barred most of the claims in *Gonzalez*.[465] The U.S. Supreme Court unanimously reversed the Ninth Circuit's decision in *Taamneh*, holding that the plaintiffs had not stated a claim under the ATA because they failed to show "any concrete nexus between defendants' services" and the attack.[466] On the same day, the Court declined to address the Ninth Circuit's holding regarding Section 230 in *Gonzalez*, instead remanding the case for reconsideration in light of *Taamneh*.[467] Thus the Court effectively sidestepped the question of whether Section 230 bars platform liability for algorithmic amplification of user-published content by resolving one case on ATA grounds alone and remanding the other. ***Large Technology Companies Continue to Face VPPA-Related Litigation.*** Several lawsuits were filed in 2023 concerning companies' collection and management of users' video-related information. For example, with respect to a lawsuit relating to one major technology company's management of user video history information, a federal district court dismissed with prejudice a claim that the company's alleged retention of the plaintiff's video rental history violated the New York Video Consumer Privacy Act and the Minnesota Video Privacy Law.[468] The court observed that, like the VPPA, these state analogue statutes were meant to prevent unauthorized *disclosure* of video-related data rather than mere retention of it.[469] In another video-related case,[470] a federal court held that the plaintiff had adequately pleaded a VPPA violation by alleging that a company disclosed information about the plaintiff's online activity to his school district, which was using the company's platform for digital learning during the COVID-19 pandemic.[471] The company moved to dismiss this claim on two grounds: First, it argued that the plaintiff was not a "subscriber" within the meaning of the VPPA, since his account with the defendant was a byproduct of his relationship with the school district.[472] Second, the company argued that any disclosure of PII was permitted by the VPPA because it was done "in the regular course of business" with the school district.[473] The court rejected both arguments, finding that the plaintiff, who held an account directly with the defendant, was plausibly a subscriber.[474] The court also said it was not appropriate to decide the second issue at the motion to dismiss stage, as the company's contract with the district was not part of the court's record.[475] ***Employers May Be Potentially Liable for Failing to Secure Employees' Personally Identifiable Information.*** 2023 also saw new lawsuits focusing on employee data privacy and seeking to hold employers liable for failing to secure employees' PII or failing to implement appropriate safeguards. For example, the United States Court of Appeals for the Eleventh Circuit ruled that a plaintiff had plausibly

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

alleged a negligence claim against a former employer that failed to protect PII in the employer's possession.[476] The complaint alleges that as a condition of employment, the plaintiff and members of the proposed class were required to give the defendant certain PII like their names and Social Security numbers.[477] However, the employer did not maintain adequate security measures to protect that information, and the PII was subsequently leaked in a ransomware attack on the employer's system.[478] The court held that such an attack was reasonably foreseeable for a large employer like the defendant; that the plaintiff adequately pleaded that the former employer owed him a duty of care; and that failure to comply with standard data security practices was plausibly a breach of that duty.[479] Thus, the court allowed the plaintiff's negligence claim to move forward. Likewise, a major car manufacturer was sued for allegedly failing to protect the personal information of 75,000 current and former employees that was exposed in a data breach carried out by former employees of the company.[480] The complaint alleges that the company failed to implement or follow reasonable data security procedures as required by law, and failed to protect the sensitive information of class members from unauthorized action.[481] The case is in its early stages, and there has not yet been any dispositive-motion practice. **IV. Trends Related to Data Innovations and Governmental Data Collection A. Data-Intensive Technologies—Privacy Implications and Trends** With the continued proliferation of data-intensive technologies, big data processing and its privacy implications continued to be an area of great focus in 2023. In addition to innovations and issues pertaining to AI, which are covered in detail in Gibson Dunn's forthcoming Artificial Intelligence Legal Review, there was a renewed focus on smart cities, edge computing and privacy-enhancing technologies (PETs). ***Smart Cities.*** The trend over the past decade of cities getting "smarter" continued at a rapid clip in 2023. A "smart city" leverages technology, data-driven decision-making, and digitally connected infrastructure to optimize the quality of municipal services, promote safe and sustainable communities, and achieve operational efficiencies.[482] Most of the technologies that smart cities are currently using do not collect or process personal data. For example, smart street-lighting technologies allow cities to turn on, turn off, and dim street lights based on the time of day and weather events and smart water management technologies allow cities to detect chemicals in drinking water and wastewater systems.[483] However, given that smart city technology applications are fueled by and necessitate large scale collection and processing of data as well as government partnership with the private sector, privacy advocates and policy makers are increasingly concerned about the privacy implications of such technology. These concerns largely relate to:

- *Data security*: Smart cities can be vulnerable to cyberattacks because they rely on internet of things ("IoT") devices, which are common and often insecure targets.[484] Furthermore, local governments often lack the resources to obtain secure technologies, update them, and employ cybersecurity experts.[485] In fact, a recent survey found that nearly one-third of local governments would be unable to detect whether their systems had been hacked.[486]
- *Commercial use of data*: Smart city data may be used commercially if a city partners with a private company to pay for technologies and in exchange gives the company access to data the city collects.[487] A privacy concern arises if the city shares sensitive data with private partners.
- *Government surveillance*: Some privacy advocates are concerned that governments will use smart city technologies to surveil individuals by obtaining data the government could not otherwise compel access to or by pulling data from different sources to build behavior profiles on individual residents.[488] Critics assert that cities are already theoretically able to aggregate enough data from smart city technologies to build detailed behavior profiles on their residents.[489] Ultimately, these debates may be settled by courts, which will decide if these data collection practices violate U.S. privacy laws or the Fourth Amendment.[490]

Although there has not been any legislation seeking to specifically regulate smart city technologies, many of the existing or pending privacy regulations are potentially applicable. However, as smart city technologies, particularly those implicating personal

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

information or sensitive data, continue to grow in number and capability, we expect to see more specific legislation targeting such technology and use cases. ***Edge Computing*.** The enormous volume of data being generated and processed by data-intensive technologies—e.g., IoT devices—has strained traditional computing models. This has led organizations to increasingly embrace "edge computing"—an emerging decentralized computing paradigm where data is processed closer to where it is generated, thus allowing processing of greater data volumes at greater speed.[491] Experts predict that spending on edge technology will continue to soar.[492] Due to deployment of strong internet infrastructures and a growing awareness of the importance of IoT across industries, the edge computing market is estimated to grow at a compound annual growth rate of 21.6% to hit an estimated $132.11 million in 2028.[493] The number of endpoint devices in use is also expected to skyrocket, with estimates of up to 55.7 billion total IoT devices deployed worldwide in the next few years.[494] Telecommunication companies are expected to play a large role in the growth of edge computing, as their widespread infrastructure and expansive reach position them well, literally (based on their close physical proximity to potential customers) and figuratively, to tap the edge computing market.[495] Although the rise of edge computing is largely a function of the benefits to data processing speed and volume, edge computing has important data privacy and security benefits. For example, edge computing can mitigate some of the privacy risks innate to centralized storage and processing,[496] by diffusing data and thus reducing the scope and impact of a data breach. Edge computing may also reduce the incentives for malicious actors, as an edge device with one or a few users' data is a less desirable target than a cloud database with millions of users' data.[497] However, by the same token, storing and processing data on devices outside of a centralized corporate network potentially makes the data less secure, given that personal edge devices are often less secure than corporate devices.[498] Some commentators have also suggested that edge computing may be an effective compliance tool, particularly with respect to cross-border data transfer laws. For example, one commentator believes that corporations will be able to use edge computing to manage personal data in adherence with local privacy laws by "placing certain locali[z]ed proxy policies that will not allow certain types of data to leave that legal jurisdiction."[499] Traces of this can be found in the EU's federated cloud infrastructure model, GAIA-X, which aims to let national governments apply local laws to cloud-hosted data.[500] Given the rapid proliferation of data-intensive technologies, we expect organizations to continue to focus on alternative computing paradigms like edge computing, which will bring new benefits and challenges for data privacy and security. **B. Emerging Privacy Enhancing Technologies (PETs)** In March 2023, the White House Office of Science and Technology Policy ("OSTP") published its "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics." In sum, the report and strategy calls for development and implementation of PETs in order to mitigate the privacy risks inherent in, and thus unlock the innovative and economic benefits of, large-scale data processing.[501] Examples of PETs include:

- *Homomorphic encryption:* Homomorphic encryption is a differential privacy technique (adding noise to the data to prevent an adversary from determining whether any individual's data was or was not included in the original dataset)[502] that allows computing over encrypted data to produce results in an encrypted form.[503] In other words, the data retains its relevant statistical characteristics for analysis, while hiding the data itself.[504] Then, only authorized users can extract the result from its encrypted format or see the original data.[505] However, homomorphic encryption is currently somewhat limited by higher computational costs and time.[506]
- *Secure multi-party computation:* Secure multi-party computation allows several parties to simultaneously perform agreed-upon computations over their data, while permitting each individual entity to learn only the final output.[507] Accordingly, distributed datasets can be computed over without revealing the source data.[508] However, the requirement of joint collaboration can lead to higher communication and computational costs, making it difficult to scale.[509]
- *Federated learning:* Federated learning allows multiple entities to collaborate and

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

build machine-learning algorithms to process data on edge devices, such as smartphones.[510] Accordingly, the underlying data is not aggregated. Instead, the locally trained models are aggregated in the cloud.[511] In this way, participants do not have to share their raw data, providing inherent privacy protection. However, federated learning has recently been shown to be vulnerable to model inversion attacks.[512] Research into closing these vulnerabilities and creating privacy-preserving federated learning is ongoing.[513]

- *Zero-knowledge proof:* Zero-knowledge proof allows one party, the "prover," to offer proof to another party, the "verifier," that a statement is true without revealing any sensitive information.[514] Some digital assets use this technique to prove statements about transactions without revealing additional metadata,[515] and neural networks are using zero-knowledge proof schemes to show that prediction tasks are being carried out, without disclosing any information about the model itself.[516] However, zero-knowledge proof currently has some cost and scalability limitations.[517]

According to the OSTP report, the impetus for a national strategy on PETs is the White House's belief that large-scale data processing is crucial for innovation and the economy. However, given the complex domestic and international regulatory landscape, the White House recognizes that inherent in such processing are significant privacy risks for data subjects and organization data subjects and organizations.[518] Accordingly, the strategy calls for the adoption of PETs, which can mitigate the privacy risks of large-scale data processing and thus unlock the benefits of data processing to fuel innovation and the economy. The OSTP report enumerates 16 recommendations across five strategic priorities to advance the development and use of PETs.[519] Importantly, the report specifically calls for the use of secure multi-party computation and zero-knowledge proofs, as well as increased public and private sector partnership and U.S. partnerships/collaboration with foreign governments. In the absence of a comprehensive federal privacy law and/or regulations specifically focused on privacy-preserving technologies, the OSTP's strategy signifies what may be the beginning of a burgeoning national standard for the development and use of PETs. **C. Governmental Data Collection *EU-US Data Privacy Framework.*** In July 2023, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework, concluding that U.S. protection of cross-border data transfers is comparable to the protection offered by the EU.[520] Speaking during a press conference announcing adoption of the U.S. adequacy decision, EU justice commissioner Didier Reynders said, "[w]ith the adoption of the adequacy decision, personal data can now flow freely and safely from the European Economic Area to the United States without any further conditions or authorizations."[521] The decision resolved the legal uncertainty surrounding exports of EU users' personal data by U.S. companies that had existed since the Court of Justice of the European Union invalidated the EU-U.S. Privacy Shield in 2020.[522] However, legal challenges are expected, with critics claiming that the Data Privacy Framework merely "paper[s] over the same fundamental legal conflict between EU privacy rights and U.S. surveillance powers."[523] Nonetheless, Reynders emphasized that the "new framework is substantially different than the EU-U.S. Privacy Shield as a result of the Executive Order issued by President Biden [in 2022]" and highlighted the reworked redress mechanism that will boast "an independent and impartial tribunal that is empowered to investigate complaints lodged by Europeans and to issue binding remedial decisions."[524] Finally, Reynders cautioned U.S. technology giants that "[i]t will be for the companies to show that they're in full compliance with the GDPR [General Data Protection Regulation]."[525] On July 17, 2023, the Department of Commerce launched the new Data Privacy Framework program website, dataprivacyframework.gov.[526] The website allows U.S. companies to self-certify their participation in and commitment to the EU-U.S. Data Privacy Framework ("DPF"), and, optionally, the UK Extension or Swiss-U.S. DPF Principles, in order to participate in cross-border transfers of personal data. ***Government Surveillance Reform Act (GSRA).*** In November 2023, a bipartisan group of senators introduced the Government Surveillance Reform Act ("GSRA"), which would reform the Foreign Intelligence Act ("FISA") and amend the Electronic Communications Privacy Act

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

("ECPA"). Importantly, the GSRA proposes significant restrictions on government surveillance and access to data—including, among other things, (i) protecting Americans from warrantless backdoor searches, (ii) requiring warrants for Americans' location data, web browsing and search records, and vehicle data, (iii) restricting government collection of Americans' information as part of large datasets and prohibiting the government from purchasing Americans' data from data brokers, and (iv) prohibiting the collection of Americans' domestic communications.[527] FISA, Section 702 was set to expire at the end of 2023,[528] but Congress approved a short-term extension in December 2023.[529] Under Section 702, the government could collect communications by non-Americans located abroad, without a warrant.[530] However, the private phone calls, emails, and text messages of U.S. persons were captured by the blanket surveillance techniques deployed under Section 702.[531] In response, several lawmakers vowed not to reauthorize Section 702 without "significant reforms."[532] The GSRA would ban officials from conducting searches for Americans' communications unless they first obtain a warrant in a criminal investigation or a FISA Title I order in a foreign intelligence investigation.[533] The new warrant requirement would provide for narrow exceptions in cases of: (1) consent, (2) exigent circumstances, or (3) a government attempt to identify targets of cyberattacks by searching for malicious code embedded in Americans' communications.[534] The GSRA would also significantly overhaul the ECPA—which addresses wiretapping, access to stored electronic communications, and other information-collection devices.[535] These changes would alter the rights and obligations of entities already covered by the ECPA and expand the reach of the ECPA to entities not currently subject to it.[536] The GSRA would:

- Expand the scope of companies subject to the ECPA to include any online service provider.[537] The GSRA would add a new category of service providers—broadly defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server"[538]—to the Stored Communications Act's ("SCA") provision governing compelled disclosures to governmental entities.[539]
- Effectively codify the Sixth Circuit's decision in *Warshak v. United States*, 631 F.3d 266 (6th Cir. 2010), which held that law enforcement must obtain a warrant to compel the disclosure of the contents of user communications.[540] Further, the GSRA would effectively codify *Carpenter v. United States*, 138 S. Ct. 2206 (2018), by requiring law enforcement to obtain a warrant to compel the disclosure of location information, web browsing records, online search queries, and covered vehicle data.[541]
- Prohibit the government from purchasing the personal data of U.S. persons (U.S. citizens and lawful permanent residents) or people reasonably believed to be located inside the United States.[542]
- Exempt congressional subpoenas from the ECPA, allowing political officials to subpoena the communications and personal data of U.S. persons without any statutory protection.[543]

Dueling Surveillance Bills in the U.S. House of Representatives. In December 2023, the House postponed a planned vote on two competing surveillance bills under a procedural rule called "Queen of the Hill," whereby the bill with the most votes is sent to the Senate.[544] The House Intelligence Committee advanced the first bill, the FISA Reform and Reauthorization Act of 2023, which faced backlash from privacy rights groups.[545] More than 50 organizations signed a letter demanding the bill's rejection.[546] By contrast, the second bill, proposed by the House Judiciary Committee, entitled The Protect Liberty and End Warrantless Surveillance Act, received support from privacy advocates.[547] Both bills are still pending in the House. **V. Conclusion** In 2023, the privacy and cybersecurity landscape in the U.S. was defined by an expansion of 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 AI and IoT; the unrelenting

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

cyber threat posed by malicious actors; and related litigation arising from these trends. We expect these trends to continue in 2024 as existing technologies and use cases take hold and new ones emerge. In the absence of comprehensive federal legislation (which is unlikely in an election year), we expect federal and state agencies to continue to lead the charge on the regulatory front and aggressively pursue enforcement actions against companies and individuals. We will continue to track and analyze these developments in the year ahead. _____ [1] Cal. Civ. Code § 1798.100 *et seq.* [2] Va. Code Ann. §§ 59.1-575 to 59.1-585. [3] Colo. Rev. Stat. Ann. § 6-1-1308. [4] Conn. Gen. Stat. Ann. § 42-520. [5] Utah Code §§ 13-61-101 to 13-61-404. [6] S.B. 262, 125 Reg. Sess. (Fla. 2023) (to be codified in Fla. Stat. § 501.701-22). [7] H.B. 4, 88 Reg. Sess. (Tex. 2023) (to be codified in Tex. Bus. & Com. Code §§ 541.001 to 541.205). [8] S.B. 618, 82 Leg. Assemb., Reg. Sess. (Or. 2023) (to be codified in Or. Laws Ch. 369). [9] S.B. 384, 68 Reg. Sess. (Mont. 2023) (to be codified in Mont. Code § 30-14-2801 to 30-14-2817). [10] S.F. 262, 89th Gen. Assemb., Reg. Sess. (Iowa 2023) (to be codified in Iowa Code § 715D.1 to 715D.9). [11] H.B. 154, 152 Gen. Assemb., Reg. Sess. (Del. 2023) (to be codified in 6 Del. Code § 12D). [12] S.B. 332, 220 Leg. Assemb., Reg. Sess. (N.J. 2023). [13] H.B. 1181; S.B. 73, 112 Gen. Assemb., Reg. Sess. (Tenn. 2023) (to be codified in Tenn. Code §§ 47-18-3301 to 47-18-3315). [14] S.B. 5, 123 Gen. Assemb., Reg. Sess. (Ind. 2023) (to be codified in Ind. Code §§ 24-15-1-1 to 24-15-11-2). [15] Notably, under the NJDPA, "financial information" is included as a form of sensitive data, which is defined as including "a consumer's account number, account log-in, financial account, or credit or debit number, in combination in combination with any required security code, access code, or password that would permit access to a consumer's financial account." [16] Under Civil Code section 1798.150, the damages available for a private right of action to pursue statutory damages between $100 and $750 per consumer per incident or actual damages, whichever is greater, as well as injunctive or declaratory relief, and "any other relief the court deems proper." A number of limitations also exist. For example, under Section 1798.150(b), a consumer must give a business an opportunity to "cure" the alleged violation by sending written notice prior to filing suit. If cured within 30 days and the consumer receives "an express written statement" indicating that the violations have been cured and shall not recur, a claim for statutory damages cannot be pursued. [17] *Protecting Washingtonians' Personal Health Data and Privacy*, Wash. Att'y Gen., https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy . [18] Wash. Rev. Code § 19.373.010(23). [19] *Id*. § 19.373.010(23). [20] *Id*. §§ 19.373.010(28), 19.373.030(2). [21] *Id*. § 19.373.010(8)(a). [22] *Id*. § 19.373.010(8)(b). [23] *Id*. § 19.373.010(8)(c). [24] *Id.* [25] *Protecting Washingtonians' Personal Health Data and Privacy*, Wash. Att'y Gen., https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy . [26] Wash. Rev. Code §§ 19.373.020; 19.373.030. [27] *Id*. §§ 19.373.010(6)(a); 19.373.030. [28] *Id*. § 19.373.040(a)–(c). [29] *Id*. § 19.373.090. [30] *Id.* § 19.255.040. [31] *Id.* [32] Mont. Code § 30-23-102(4). [33] *Id*. § 30-23-102(6). [34] *Id*. § 30-23-104(1)–(2). [35] *Id*. § 330-23-104(5). [36] *Id*. § 30-23-106. [37] Press Release, Senator Josh Becker, *Governor Newsom Signs First in the Nation Bill to Protect Consumers' Data from Unknown Third Parties* (Oct. 10, 2023), https://sd13.senate.ca.gov/news/press-release/october-10-2023/governor-newsom-signs-first-in-the-nation-bill-to-protect. [38] Cal. Civ. Code §§ 1798.99.84; 1798.99.86(a)–(b). [39] *Id*. § 1798.99.86(c)–(d). [40] *Id*. § 1798.99.86(d)(2). [41] *Id*. § 1798.99.86(a)(3). [42] *Id*. § 1798.99.86(e)(1). [43] *Id*. § 1798.99.80(c). [44] *Id*. § 1798.99.80(c)(1)(4). [45] N.Y. Dep't of Fin. Servs., *Cybersecurity Resource Center*, https://www.dfs.ny.gov/industry_guidance/cybersecurity. [46] N.Y. Dep't of Fin. Servs., *Enforcement and Discipline*, https://dfs.ny.gov/industry_guidance/enforcement_actions. [47] Press Release, Utah Governor Spencer J. Cox, *Gov. Cox Signs Bills Focused on Social Media and Youth Mental Health in Utah* (Mar. 23, 2023), https://governor.utah.gov/2023/03/23/gov-cox-signs-bills-focused-on-social-media-in-utah/. [48] Utah Code § 13-63-101, *et seq.* [49] *Id.* §§ 13-63-201–301. [50] *Id.* § 13-63-301. [51] *NetChoice, LLC v. Reyes*, No. 2:23-cv-00911 (D. Utah); *Zoulek v. Hass*, No. 2:24-cv-00031 (D. Utah). [52] *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155, at *7 (W.D. Ark. Aug. 31, 2023). [53] *Id.* at *13. [54] *Id.* at *17, 40–41. [55] *Alario v. Knudsen*, No. CV 23-56-M-DWM, 2023 WL 8270811 (D. Mont. Nov. 30, 2023). [56] *Id.* at *4. [57] American Data Privacy and Protection Act ("ADPPA"),

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

H.R. 8152, 117th Cong. (2022). [58] *Id*. §§ 101(a)–(b), 103(a). [59] *Id*. § 207(a)(1). [60] *Id.* §§ 207(b), 401, 402(a). [61] *Id*. § 403(a). [62] *Id*. § 404(b)(1). [63] *See Innovation, Data, and Commerce Subcommittee Hearing: "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information,"* U.S. House Energy & Commerce Comm. (Apr. 27, 2023), https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-addressing-america-s-data-privacy-shortfalls-how-a-national-standard-fills-gaps-to-protect-americans-personal-information; *Innovation, Data, and Commerce Subcommittee Hearing: "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy,"* U.S. House Energy & Commerce Comm. (Mar. 1, 2023), https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-promoting-u-s-innovation-and-individual-liberty-through-a-national-standard-for-data-privacy. [64] Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023); *see also* Press Release, White House, *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence* (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence. [65] *Remarks of President Joe Biden – State of the Union Address as Prepared for Delivery*, White House (Feb. 7, 2023), https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/07/remarks-of-president-joe-biden-state-of-the-union-address-as-prepared-for-delivery. [66] *See* Eric McDaniel, *Congress Passed So Few Laws This Year That We Explained Them All in 1,000 Words*, NPR (Dec. 22, 2023), https://www.npr.org/2023/12/22/1220111009/congress-passed-so-few-laws-this-year-that-we-explained-them-all-in-1-000-words; Müge Fazlioglu, *US Federal Privacy Legislation Tracker: Introduced in the 118th Congress (2023-2024)*, IAPP (last updated Sept. 2023), https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf. [67] Müge Fazlioglu, *U.S. Privacy Legislation in 2023: Something Old, Something New?*, IAPP (July 26, 2023), https://iapp.org/news/a/u-s-federal-privacy-legislation-in-2023-something-old-something-new. [68] Press Release, U.S. Senate Judiciary Comm., *Durbin, Graham Announce January 2024 Hearing with Five Big Tech CEOs on their Failure to Protect Children Online* (Nov. 29, 2023), https://www.judiciary.senate.gov/press/releases/durbin-graham-announce-january-2024-hearing-with-five-big-tech-ceos-on-their-failure-to-protect-children-online; *Full Committee Hearing: "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms,"* U.S. House Energy & Commerce Comm. (Mar. 23, 2023), https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms. [69] Kids Online Safety Act, S. 1409, 118th Cong. (2023). [70] Children and Teens' Online Privacy Protection Act, S. 1418, 118th Cong. (2023). [71] Informing Consumers about Smart Devices Act, S. 90, 118th Cong. (2023). [72] Stop Spying Bosses Act, S. 262, 118th Cong. (2023). [73] UPHOLD Privacy Act of 2023, S. 631, 118th Cong. (2023). [74] DELETE Act, H.R. 4311, 118th Cong. (2023). [75] Data Care Act of 2023, S. 744, 118th Cong. (2023). [76] Online Privacy Act of 2023, H.R. 2701, 118th Cong. (2023). [77] Federal Cybersecurity Vulnerability Reduction Act of 2023, H.R. 5255, 118th Cong. (2023). [78] Modernizing the Acquisition of Cybersecurity Experts Act of 2023, H.R. 4502, 118th Cong. (2023). [79] Federal Cybersecurity Workforce Expansion Act, S. 2256, 118th Cong. (2023). [80] *See* Press Release, White House, *President Biden Recognizes Actions by Private Sector Ticketing and Travel Companies to Eliminate Hidden Junk Fees and Provide Millions of Customers with Transparent Pricing* (June 15, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/15/president-biden-recognizes-actions-by-private-sector-ticketing-and-travel-companies-to-eliminate-hidden-junk-fees-and-provide-millions-of-customers-with-transparent-pricing/. *See also* Press Release, White House, *FACT SHEET: Executive Order on Promoting Competition in the American Economy* (July 9, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/. [81] Trade Regulation Rule on Unfair or Deceptive Fees, 88 Fed. Reg. 77420 (Nov. 9, 2023), https://www.federalregister.gov/documents/2023/11/09/2023-24234/trade-regulation-rule-

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

on-unfair-or-deceptive-fees; Trade Regulation Rule on Unfair or Deceptive Fees, 89 Fed. Reg. 38 (Jan. 2, 2024). [82] Christine Wilson, *Letter to President Joseph R. Biden* (Mar. 2, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p180200wilsonresignationletter.pdf. [83] *See* Press Release, White House, *President Biden Announces Nominees to Bipartisan Boards and Commissions* (July 3, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/03/president-biden-announces-nominees-to-bipartisan-boards-and-commissions. [84] Melissa Holyoak, Statement Before the U.S. Senate Committee on Commerce, Science, and Transportation (Sep. 20, 2023), https://www.commerce.senate.gov/services/files/51CBECA7-1810-4CCD-8046-0AE99CA34CC4. [85] Hawley Holds Nominees, Calls for Further Evaluation of McConnell Nominees, Senate Office of Josh Hawley (Dec. 20, 2023), https://www.hawley.senate.gov/hawley-holds-nominees-calls-further-evaluation-mcconnell-nominees. [86] Lina Khan, *Lina Khan: We Must Regulate A.I. Here's How*, New York Times (May 3, 2023), https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html. [87] Michael Atleson, *Keep Your AI Claims in Check*, Federal Trade Commission (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check. [88] Michael Atleson, *Chatbots, Deepfakes, and Voice Clones: AI Deception for Sale*, Federal Trade Commission (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale. [89] *Id.* [90] *Id.* [91] Michael Atleson, *The Luring Test: AI and the Engineering of Consumer Trust*, Federal Trade Commission (May 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust. [92] Michael Atleson, *Watching the Detectives: Suspicious Marketing Claims for Tools that Spot AI-Generated Content*, Federal Trade Commission (May 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/watching-detectives-suspicious-marketing-claims-tools-spot-ai-generated-content. [93] Alex Gaynor, Security Principles: Addressing Underlying Causes of Risk in Complex Systems, Federal Trade Commission (February 1, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems. [94] *Id.* [95] *Id.* [96] Samuel Levine, Chief, Federal Trade Commission, *Remarks of Chief Samual Levine at the Consumer Data Industry Association Law and Industry Conference* (September 21, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/cdia-sam-levine-9-21-2023.pdf. [97] Mike Swift, *US FTC still pondering 'commercial surveillance' rulemaking, Slaughter tells tech industry*, MLex (Jan. 10, 2024), https://content.mlex.com/#/content/1535579. [98] Press Release, Federal Trade Commission, *FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay $245 Million for Tricking Users into Making Unwanted Charges* (Mar. 14, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making. [99] 15 U.S.C. § 45(a). [100] Complaint, *FTC v. Ring LLC*, Case No. 1:23-cv-1549 (May 31, 2023). [101] Proposed Stipulated Order, *FTC v. Ring LLC*, Case No. 1:23-cv-1549 (May 31, 2023); Press Release, Federal Trade Commission, *FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras* (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users. [102] Notices of Penalty Offenses, Federal Trade Commission, https://www.ftc.gov/enforcement/penalty-offenses. [103] Press Release, Federal Trade Commission, *FTC Warns Tax Preparation Companies About Misuse of Consumer Data* (Sep. 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-warns-tax-preparation-companies-about-misuse-consumer-data. [104] Complaint, *U.S. v. Amazon.com, Inc., and Amazon.com Services LLC*, Case No. 2:23-cv-00811 (May 31, 2023). [105] *Amazon Alexa*, Federal Trade Commission (July 21, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/amazon-alexa. [106] Press Release, Federal Trade Commission, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising. [107] Press Release, Federal Trade Commission, *FTC Warns Health Apps and Connected Device Companies to*

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Comply With Health Breach Notification Rule (Sep. 21, 2023), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health-breach-notification-rule. [108] Press Release, Federal Trade Commission, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising* (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising. [109] Health Breach Notification Rule, 88 Fed. Reg. 37819, 37839 (June 9, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule; *see also* Press Release, Federal Trade Commission, *FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule* (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule. [110] Press Release, Federal Trade Commission, *FTC Finalizes Order with 1Health.io Over Charges it Failed to Protect Privacy and Security of DNA Data and Unfairly Changed its Privacy Policy* (Sep. 7, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-finalizes-order-1healthio-over-charges-it-failed-protect-privacy-security-dna-data-unfairly. [111] *FTC v. Rite Aid Corp*., No. 2:23-cv-05023 (E.D. Pa. Dec. 19, 2023). [112] Press Release, Federal Trade Commission, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data. [113] Press Release, Federal Trade Commission, *FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches* (October 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches. [114] Press Release, Federal Trade Commission, *Compliance deadline for certain revised FTC Safeguards Rule provisions extended to June 2023* (November 15, 2022), https://www.ftc.gov/business-guidance/blog/2022/11/compliance-deadline-certain-revised-ftc-safeguards-rule-provisions-extended-june-2023. [115] *Id.* [116] Press Release, Federal Trade Commission, *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches* (Oct. 27, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data. [117] Press Release, Federal Trade Commission, *FTC Proposes Strengthening Children's Privacy Rule to Further Limit Comanies' Ability to Monetize Children's Data* (December 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens. [118] *Id.* [119] *Id.* [120] *Id.*; Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034 (Jan. 11, 2024). https://www.federalregister.gov/documents/2024/01/11/2023-28569/childrens-online-privacy-protection-rule. [121] Press Release, Federal Trade Commission, *FTC Seeks Comment on New Parental Consent Mechanism Under COPPA* (July 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-seeks-comment-new-parental-consent-mechanism-under-coppa. [122] *Id.* [123] Press Release, Federal Trade Commission, *FTC Will Require Microsoft to Pay $20 million over Charges it Illegally Collected Personal Information from Children without Their Parents' Consent* (June 5, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information. [124] *Id.* [125] Press Release, Federal Trade Commission, *FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data* (May 3, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data. [126] *Id.* [127] *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, Federal Trade Commission (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf. [128] Press Release, Federal Trade Commission, *FTC to Host Identity Authentication Workshop* (Feb. 21, 2007) https://www.ftc.gov/news-events/news/press-releases/2007/02/ftc-host-identity-authentication-w; *You Don't Say: An FTC Workshop on Voice Cloning Technologies*,

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Federal Trade Commission (Jan. 28, 2020), https://www.ftc.gov/newsevents/events/2020/01/you-dont-say-ftc-workshop-voice-cloning-technologies; *Face Facts: A Forum on Facial Recognition Technology*, Federal Trade Commission (Dec. 8, 2011), https://www.ftc.gov/newsevents/events/2011/12/face-facts-forum-facial-recognition-technology; *Facing Facts: Best Practices for Common Uses of Facial Recognition Technology*, Federal Trade Commission (Oct. 2012), https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies. [129] *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, Federal Trade Commission (May 18, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf. [130] *Id.* [131] Press Release, Federal Trade Commission, *Rite Aid Banned From Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards* (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without. [132] Press Release, Consumer Financial Protection Bureau, *CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking* (Oct. 19, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/. [133] *Id.* [134] *See id.*; Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74809 (Oct. 31, 2023) (to be codified at 12 C.F.R. pts. 1001, 1033), https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights. [135] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74796 (Oct. 31, 2023) (to be codified at 12 C.F.R. pts. 1001, 1033), https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights. [136] 12 U.S.C. § 5533(a). [137] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74803 (Oct. 31, 2023) (to be codified at 12 C.F.R. pts. 1001, 1033), https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights. [138] *Id.* at 74809. [139] *Id.* at 74832. [140] *Id.* at 74833. [141] *Id.* at 74874. [142] *Id.*; Press Release, Consumer Financial Protection Bureau, *Prepared Remarks of CFPB Director Rohit Chopra on the Proposed Personal Financial Data Rights Rule* (Oct. 19, 2023), https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-on-the-proposed-personal-financial-data-rights-rule/. [143] Press Release, Consumer Financial Protection Bureau, *CFPB Proposes New Federal Oversight of Big Tech Companies and Other Providers of Digital Wallets and Payment Apps* (Nov. 7, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-new-federal-oversight-of-big-tech-companies-and-other-providers-of-digital-wallets-and-payment-apps/. [144] Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, 88 Fed. Reg. 80197, 80199, 80204 (Nov. 17, 2023) (to be codified at 12 C.F.R. pt. 1090), https://www.federalregister.gov/documents/2023/11/17/2023-24978/defining-larger-participants-of-a-market-for-general-use-digital-consumer-payment-applications. [145] Press Release, Consumer Financial Protection Bureau, *CFPB Proposes New Federal Oversight of Big Tech Companies and Other Providers of Digital Wallets and Payment Apps* (Nov. 7, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-new-federal-oversight-of-big-tech-companies-and-other-providers-of-digital-wallets-and-payment-apps/. [146] *Id.* [147] Press Release, Consumer Financial Protection Bureau, *CFPB Launches Inquiry Into the Business Practices of Data Brokers* (Mar. 15, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/. [148] Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16951, 16952 (Mar. 21, 2023), https://www.federalregister.gov/documents/2023/03/21/2023-05670/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection. [149] Press Release, Consumer Financial Protection Bureau, *Remarks of CFPB Director*

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices (Aug. 15, 2023), https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/. [150] *Id.*; *see also* 15 U.S.C. § 1681b. [151] *Id*. [152] *Id*. [153] Press Release, Consumer Financial Protection Bureau, *CFPB and Federal Partners Confirm Automated Systems and Advanced Technology Not an Excuse for Lawbreaking Behavior* (Apr. 25, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-federal-partners-confirm-automated-systems-advanced-technology-not-an-excuse-for-lawbreaking-behavior/. [154] Press Release, Consumer Financial Protection Bureau, *CFPB Issue Spotlight Analyzes "Artificial Intelligence" Chatbots in Banking* (June 3, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-issue-spotlight-analyzes-artificial-intelligence-chatbots-in-banking. [155] Rohit Chopra, *Algorithms, Artificial Intelligence, and Fairness in Home Appraisals*, CFPB Blog (June 1, 2023), https://www.consumerfinance.gov/about-us/blog/algorithms-artificial-intelligence-fairness-in-home-appraisals/. [156] Quality Control Standards for Automated Valuation Models, 88 Fed. Reg. 40638, 40638 (June 21, 2023), https://www.federalregister.gov/documents/2023/06/21/2023-12187/quality-control-standards-for-automated-valuation-models. [157] Rohit Chopra, *Algorithms, Artificial Intelligence, and Fairness in Home Appraisals*, CFPB Blog (June 1, 2023), https://www.consumerfinance.gov/about-us/blog/algorithms-artificial-intelligence-fairness-in-home-appraisals/. [158] Quality Control Standards for Automated Valuation Models, 88 Fed. Reg. 40638, 40638 (June 21, 2023), https://www.federalregister.gov/documents/2023/06/21/2023-12187/quality-control-standards-for-automated-valuation-models. [159] Press Release, Consumer Financial Protection Bureau, *CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence* (Sept. 19, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/. [160] *Id.* [161] Press Release, SEC, *SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information* (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-51. [162] *Id*. [163] *Id*. [164] *Id*. [165] A Small Entity Compliance Guide, SEC, *Cybersecurity Risk Management Strategy, Governance, and Incident Disclosure* (Nov. 14, 2023), https://www.sec.gov/corpfin/secg-cybersecurity#_ftn1. [166] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, 88 Fed. Reg. 51896, 51899. [167] *Id.* [168] *Id.* [169] *Id.* [170] *Id*. at 51924. [171] *Id*. at 51898–51899. [172] *Id*. at 51945. [173] *Id*. at 51909–51910. [174] The rule also includes another exemption that only applies to companies subject to the Federal Communications ("FCC") notification rule for breaches of customer proprietary network information ("CPNI"). A more detailed description of this exception is outlined in Gibson Dunn's July 31, 2023 update. [175] *Id*. [176] DOJ, *Department of Justice Material Cybersecurity Incident Delay Determinations* (Dec. 12, 2023), https://www.justice.gov/media/1328226/dl?inline. [177] *Id*. [178] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Exchange Act Release, 88 Fed. Reg. 51896, 51899. [179] *Id*. [180] *Id*. at 51913. [181] *Id*. [182] *Id*. [183] *Id*. at 51914. [184] The Commission's Privacy Act Regulations, 88 Fed. Reg. 65807, 65808. [185] *Id*. at 65808–09. [186] Press Release, SEC, *SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds* (Feb. 9, 2022), https://www.sec.gov/news/press-release/2022-20. [187] *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, 87 Fed. Reg. 13524 (published Mar. 9, 2022) (to be codified at 17 C.F.R. pts. 230, 232, 239, 270, 274, 275, 279), https://www.federalregister.gov/documents/2022/03/09/2022-03145/cybersecurity-risk-management-for-investment-advisers-registered-investment-companies-and-business. [188] SEC, *Agency Rule List - Fall 2023*, https://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3235&csrf_token=28A8C6498A23E2932F2D7BB0618F4AA9746D20D66D0E1500674B7BEBFD26693EFE119AEDE913D6851EE65F43B418CC81FFA8. [189] SEC, *View Rule* (last visited, Jan. 26, 2023),

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=3235-AN15. [190] SEC, *2024 Examination Priorities* (Oct. 16, 2023), https://www.sec.gov/files/2024-exam-priorities.pdf. [191] Press Release, SEC, *SEC Division of Examinations Announces 2024 Priorities*, https://www.sec.gov/news/press-release/2023-222/. [192] SEC, *SEC Enforcement Results for FY23* (last modified, Jan. 22, 2024), https://www.sec.gov/newsroom/enforcement-results-fy23. [193] SEC, *SEC Enforcement Results for FY23* (last modified, Jan. 22, 2024), https://www.sec.gov/newsroom/enforcement-results-fy23. [194] *Id.* [195] *Id.* [196] Press Release, SEC, *SEC Charges Virtu for False and Misleading Disclosures Relating to Information Barriers* (September 12, 2023), https://www.sec.gov/news/press-release/2023-176. [197] *Id.* [198] *Id.* [199] *Id.* [200] Press Release, SEC, *SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors* (March 9, 2023), https://www.sec.gov/news/press-release/2023-48. [201] *Id.* [202] *Id.* [203] *Id.* [204] *Id.* [205] Press Release, SEC, *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures* (Oct. 30, 2023), https://www.sec.gov/news/press-release/2023-227; *see also* Complaint ¶ 1, *SEC v. SolarWinds Corp.*, No. 1:23-9518 (S.D.N.Y. Oct. 30, 2023), ECF No. 1. [206] Press Release, SEC, *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures* (Oct. 30, 2023), https://www.sec.gov/news/press-release/2023-227. [207] *Id.* [208] *Id.* [209] *Id.* [210] *Id.* [211] *Id.* [212] *Id.* [213] *Id.* [214] *Id.* [215] Press Release, Department of Health and Human Services, *HHS Announces New Divisions Within the Office for Civil Rights to Better Address Growing Need of Enforcement in Recent Years* (Feb. 27, 2023), https://www.hhs.gov/about/news/2023/02/27/hhs-announces-new-divisions-within-office-civil-rights-better-address-growing-need-enforcement-recent-years.html. [216] *Id.* [217] *Id.* [218] *Id*. [219] Press Release, Department of Health and Human Services, *HHS Finalizes Rule to Advance Health IT Interoperability and Algorithm Transparency* (Dec. 13, 2023), https://www.hhs.gov/about/news/2023/12/13/hhs-finalizes-rule-to-advance-health-it-interoperability-and-algorithm-transparency.html; *see also* Press Release, Department of Health and Human Services, *HHS Proposes New Rule to Further Implement the 21st Century Cures Act* (Apr. 11, 2023), https://www.hhs.gov/about/news/2023/04/11/hhs-propose-new-rule-to-further-implement-the-21st-century-cures-act.html. [220] *Id*. [221] Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, *Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing*, 45 C.F.R. § 170, https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and. [222] *Id*.; *see also* Department of Health and Human Services, *Telehealth policy updates* (Nov. 9, 2023), https://telehealth.hhs.gov/providers/telehealth-policy/telehealth-policy-updates. [223] Press Release, Department of Health and Human Services, *Fact Sheet: End of the COVID-19 Public Health Emergency* (May 9, 2023), https://www.hhs.gov/about/news/2023/05/09/fact-sheet-end-of-the-covid-19-public-health-emergency.html. [224] *Id.* [225] Department of Health and Human Services, *Telehealth Policy Changes After the COVID-19 Public Health Emergency* (Dec. 19, 2023), https://telehealth.hhs.gov/providers/telehealth-policy/policy-changes-after-the-covid-19-public-health-emergency. [226] Press Release, Department of Health and Human Services, *HHS Office for Civil Rights and the Federal Trade Commission Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies* (July 20, 2023), https://www.hhs.gov/about/news/2023/07/20/hhs-office-civil-rights-federal-trade-commission-warn-hospital-systems-telehealth-providers-privacy-security-risks-online-tracking-technologies.html. [227] *Id.* [228] FTC, *Updated FTC-HHS publication outlines privacy and security laws and rules that impact consumer health data* (Sept. 15, 2023), https://www.ftc.gov/business-guidance/blog/2023/09/updated-ftc-hhs-publication-outlines-privacy-security-laws-rules-impact-consumer-health-data. [229] Press Release, Department of Health and Human Services, *Statement from Secretary Becerra on the One Year Anniversary of the Dobbs v. Jackson Women's Health Organization Decision* (June

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

24, 2023), https://www.hhs.gov/about/news/2023/06/24/statement-secretary-becerra-one-year-anniversary-dobbs-v-jackson-womens-health-organization-decision.html. [230] *See Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215 (2022). [231] Press Release, Department of Health and Human Services, *Statement from Secretary Becerra on the One Year Anniversary of the Dobbs v. Jackson Women's Health Organization Decision* (June 24, 2023), https://www.hhs.gov/about/news/2023/06/24/statement-secretary-becerra-one-year-anniversary-dobbs-v-jackson-womens-health-organization-decision.html. [232] Press Release, Department of Health and Human Services, *HHS Proposes Measures to Bolster Patient-Provider Confidentiality Around Reproductive Health Care* (Apr. 12, 2023), https://www.hhs.gov/about/news/2023/04/12/hhs-proposes-measures-bolster-patient-provider-confidentiality-around-reproductive-health-care.html. [233] *Id.*; *see also* Regulatory Initiatives, Department of Health and Human Services, *HIPAA Privacy Rule and Reproductive Health Care* (Apr. 14, 2023), https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/index.html. [234] HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506 (proposed Apr. 17, 2023) (to be codified at 45 C.F.R. pts. 160, 164); HHS/OCR, *View Rule* (last visited Jan. 26, 2024), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0945-AA20. [235] Press Release, Department of Health and Human Services, *HHS' Office for Civil Rights Settles HIPAA Investigation of St. Joseph's Medical Center for Disclosure of Patients' Protected Health Information to a News Reporter* (Nov. 20, 2023), https://www.hhs.gov/about/news/2023/11/20/hhs-office-civil-rights-settles-hipaa-investigation-st-josephs-medical-center-disclosure-patients-protected-health-information-news-reporter.html; Department of Health and Human Services, *St. Joseph's Medical Center Resolution Agreement and Corrective Action Plan* (Aug. 22, 2023), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sjmc-ra-cap/index.html. [236] *Id*. [237] *Id.* [238] *Id.* [239] Press Release, Department of Health and Human Services, *HHS' Office for Civil Rights Settles Multiple HIPAA Complaints With Optum Medical Care Over Patient Access to Records* (Dec. 15, 2023), https://www.hhs.gov/about/news/2023/12/15/hhs-office-for-civil-rights-settles-multiple-hipaa-complaints-with-optum-medical-care-over-patient-access-to-records.html. [240] *Id.* [241] *See id.* [242] Press Release, Department of Health and Human Services, *HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking* (Feb. 2, 2023), https://www.hhs.gov/about/news/2023/02/02/hhs-office-for-civil-rights-settles-hipaa-investigation-with-arizona-hospital-system.html. [243] *Id*. [244] Press Release, Department of Health and Human Services, *HHS' Office for Civil Rights Settles First Ever Phishing Cyber-Attack Investigation* (Dec. 7, 2023), https://www.hhs.gov/about/news/2023/12/07/hhs-office-for-civil-rights-settles-first-ever-phishing-cyber-attack-investigation.html. [245] *Id.* [246] *Id*. [247] Press Release, Department of Homeland Security, *Statement from Secretary Mayorkas on President Biden's National Cybersecurity Strategy* (Mar. 2, 2023), https://www.dhs.gov/news/2023/03/02/statement-secretary-mayorkas-president-bidens-national-cybersecurity-strategy. [248] Press Release, Department of Homeland Security, *DHS Issues Recommendations to Harmonize Cyber Incident Reporting for Critical Infrastructure Entities* (Sept. 19, 2023), https://www.dhs.gov/news/2023/09/19/dhs-issues-recommendations-harmonize-cyber-incident-reporting-critical. [249] Brandon Wales, *CIRCIA at One Year: A Look Behind the Scenes*, Cybersecurity & Infrastructure Security Agency (Mar. 24, 2023), https://www.cisa.gov/news-events/news/circia-one-year-look-behind-scenes; *see also* Gibson Dunn's client alert on the Cyber Incident Reporting for Critical Infrastructure Act, https://www.gibsondunn.com/president-biden-signs-into-law-the-cyber-incident-reporting-for-critical-infrastructure-act-expanding-cyber-reporting-obligations-for-a-wide-range-of-public-and-private-entities/. [250] Press Release, Department of Homeland Security, *Joint Statement from 21 Countries and the Organization of American States Following the Department of Homeland Security Western Hemisphere Cyber Conference* (Sept. 28, 2023), https://www.dhs.gov/news/2023/09/28/joint-statement-21-countries-and-organization-american-states-following-department. [251] Press Release, Cybersecurity and Infrastructure Security Agency, *CISA and FBI Release Advisory on CL0P Ransomware Gang Exploiting MOVEit Vulnerability* (June 7, 2023), https://www.cisa.gov/news-events/news/cisa-and-fbi-release-advisory-cl0p-ransomware-gang-exploiting-moveit-vulnerability.

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

[252] Press Release, Department of Homeland Security, *Cyber Safety Review Board Releases Report on Activities of Global Extortion-Focused Hacker Group Lapsus$* (Aug. 10, 2023), https://www.dhs.gov/news/2023/08/10/cyber-safety-review-board-releases-report-activities-global-extortion-focused; Press Release, Department of Homeland Security, *Department of Homeland Security's Cyber Safety Review Board to Conduct Review on Cloud Security* (Aug. 11, 2023), https://www.dhs.gov/news/2023/08/11/department-homeland-securitys-cyber-safety-review-board-conduct-review-cloud. [253] Cybersecurity Advisory, Cybersecurity and Infrastructure Security Agency, *#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability* (Nov. 21, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a. [254] Press Release, Department of Homeland Security, *DHS Announces Additional $374.9 Million in Funding to Boost State, Local Cybersecurity* (Aug. 7, 2023), https://www.dhs.gov/news/2023/08/07/dhs-announces-additional-3749-million-funding-boost-state-local-cybersecurity. [255] Press Release, Department of Justice, *Justice Department Announces New National Security Cyber Section Within the National Security Division* (June 20, 2023), https://www.justice.gov/opa/pr/justice-department-announces-new-national-security-cyber-section-within-national-security. [256] *Id.* [257] Press Release, Department of Justice, *U.S. Department of Justice Disrupts Hive Ransomware Variant* (Jan. 26, 2023), https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant. [258] *Id.* [259] Press Release, Department of Justice, *Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service* (May 9, 2023), https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled. [260] *Id.* [261] Press Release, Department of Justice, *Qakbot Malware Disrupted in International Cyber Takedown* (Aug. 29, 2023), https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown. [262] Press Release, Department of Justice, *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant* (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant. [263] *Id.* [264] Press Release, Department of Justice, *Justice Department and Meta Platforms Inc. Reach Key Agreement as They Implement Groundbreaking Resolution to Address Discriminatory Delivery of Housing Advertisements* (Jan. 9, 2023), https://www.justice.gov/opa/pr/justice-department-and-meta-platforms-inc-reach-key-agreement-they-implement-groundbreaking. [265] *Id.* [266] *Id.*; Roy L. Austin, Jr., *An Update on Our Ads Fairness Efforts*, Meta (Jan. 9, 2023), https://about.fb.com/news/2023/01/an-update-on-our-ads-fairness-efforts/. [267] Press Release, Department of Justice, *Justice Department Files Statement of Interest in Fair Housing Act Case Alleging Unlawful Algorithm-Based Tenant Screening Practices* (Jan. 9, 2023), https://www.justice.gov/opa/pr/justice-department-files-statement-interest-fair-housing-act-case-alleging-unlawful-algorithm. [268] *Id.* [269] *Id.* [270] RESTRICT Act, S. 686, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/686/text. [271] Statements and Releases, White House, *Statement from National Security Advisor Jake Sullivan on the Introduction of the RESTRICT Act* (Mar. 7, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/07/statement-from-national-security-advisor-jake-sullivan-on-the-introduction-of-the-restrict-act/; Press Release, Department of Commerce, *Statement from U.S. Secretary of Commerce Gina Raimondo on the Introduction of the RESTRICT Act* (Mar. 7, 2023), https://www.commerce.gov/news/press-releases/2023/03/statement-us-secretary-commerce-gina-raimondo-introduction-restrict-act. [272] RESTRICT Act, S. 686, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/686/text. [273] Protecting Americans' Data From Foreign Surveillance Act of 2023, S. 1974, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/1974/text. [274] *Id.* [275] *Id.* [276] *Id.* [277] *Id.* [278] Press Release, Office of Cybersecurity, Energy Security, and Emergency Response, *DOE Announces $39 Million in Research Funding to Enhance Cybersecurity of Clean Distributed Energy Resources* (Sept. 12, 2023), https://www.energy.gov/ceser/articles/doe-announces-39-million-research-funding-enhance-cybersecurity-clean-distributed. [279] *Id.* [280] *Id.* [281] Alexandra Kelley, *Cyberattacks on Energy's National Labs Draw Lawmaker Scrutiny*, Nextgov/FCW (Feb. 2,

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

2023), https://www.nextgov.com/cybersecurity/2023/02/cyberattacks-energys-national-labs-draw-lawmaker-scrutiny/382503/. [282] Special Report, Department of Energy, *Management Challenges at the Department of Energy — Fiscal Year 2024* (Nov. 17, 2023), https://www.energy.gov/sites/default/files/2023-11/DOE-OIG-24-05.pdf. [283] *Id.* [284] Daniel Wilson, *Defense Dept. Proposes Long-Awaited Cybersecurity Rule*, Law360 (Dec. 22, 2023), https://www.law360.com/cybersecurity-privacy/articles/1780256/defense-dept-proposes-long-awaited-cybersecurity-rule. [285] *Id.* [286] *Id.* [287] Press Release, Federal Communications Commission, *Chairwoman Rosenworcel Launches Privacy and Data Protection Task Force* (June 14, 2023), https://www.fcc.gov/document/chairwoman-rosenworcel-launches-privacy-and-data-protection-task-force. [288] *Id.* [289] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019); Federal Communications Commission, *TRACED Act Implementation* (May 1, 2023), https://www.fcc.gov/TRACEDAct. [290] Limits on Exempted Calls Under the Telephone Consumer Protection Act of 1991, 88 Fed. Reg. 3668 (Jan. 20, 2023) (to be codified at 47 C.F.R. pt. 64). [291] *Id.* [292] Press Release, Federal Communications Commission, *Rosenworcel Launches Effort on AI's Impact on Robocalls and Robotexts* (Oct. 23, 2023), https://docs.fcc.gov/public/attachments/DOC-397925A1.pdf. [293] Federal Communications Commission, *FCC Launches Inquiry into AI's Impact on Robocalls and Robotexts* (Nov. 17, 2023), https://www.fcc.gov/consumer-governmental-affairs/fcc-launches-inquiry-ais-impact-robocalls-and-robotexts. [294] Federal Communications Commission, *Second Report and Order, Second Further Notice of Proposed Rulemaking in CG Docket Nos. 02-278 and 21-402, and Waiver Order in CG Docket No. 17-59* (Dec. 18, 2023), https://docs.fcc.gov/public/attachments/FCC-23-107A1.pdf. [295] *Id.* at 13–15. [296] *Id.* at 20 n.113. [297] Press Release, White House, *Biden-?Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers* (July 18, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/. [298] *Id.* [299] Press Release, Federal Communications Commission, *FCC Fact Sheet on Proposed Voluntary Cybersecurity Labeling Program for Internet-Enabled Devices* (Aug. 10, 2023), https://docs.fcc.gov/public/attachments/DOC-395909A1.pdf. [300] Press Release, Federal Communications Commission, *FCC Adopts Updated Data Breach Notification Rules To Protect Consumers* (Dec. 13, 2023), https://docs.fcc.gov/public/attachments/DOC-399090A1.pdf. [301] *Id.* [302] Press Release, Federal Communications Commission, *FCC Proposes $20M Fine for Apparently Failing to Protect Consumer Data* (July 28, 2023), https://docs.fcc.gov/public/attachments/DOC-395581A1.pdf. [303] *Id.* [304] *A New Landmark for Consumer Control Over Their Personal Information: CPPA Proposes Regulatory Framework for Automated Decisionmaking Technology*, Cal. Privacy Protection Agency (Nov. 27, 2023), https://cppa.ca.gov/announcements/2023/20231127.html; *see also Draft Automated Decisionmaking Technology Regulations*, Cal. Privacy Protection Agency (Dec. 8, 2023), https://cppa.ca.gov/meetings/materials/20231208_item2_draft.pdf. [305] *CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies*, Cal. Privacy Protection Agency (July 31, 2023), https://cppa.ca.gov/announcements/2023/20230731.html. [306] *Ahead of Privacy Day, Attorney General Bonta Focuses on Mobile Applications' Compliance with the California Consumer Privacy Act*, Cal. Att'y Gen. (Jan. 27, 2023), https://oag.ca.gov/news/press-releases/ahead-data-privacy-day-attorney-general-bonta-focuses-mobile-applications%E2%80%99. [307] *Attorney General Bonta Seeks Information from California Employers on Compliance with California Consumer Privacy Act*, Cal. Att'y Gen. (July 14, 2023), https://oag.ca.gov/news/press-releases/attorney-general-bonta-seeks-information-california-employers-compliance. [308] Complaint, *People v. Google*, Case No. 23CV422424 (Santa Clara Cnty. Super. Ct., Sept. 14, 2023), https://oag.ca.gov/system/files/attachments/press-

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

docs/Filed%20stamped%20Google%20Complaint.pdf. [309] *Attorney General James Seeks information from Madison Square garden Regarding Use of Facial Recognition Technology to Deny Entry to Venues*, N.Y. Att'y Gen. (Jan. 25, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-seeks-information-madison-square-garden-regarding-use. [310] *DFS Announces $1 million Cybersecurity Settlement with First American Title Insurance Company*, N.Y. Dept. of Fin. Servs. (Nov. 28, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202311281 [311]*Id.* [312] *AG Ferguson's lawsuit forces Google to pay nearly $40M over deceptive location tracking*, Wash. Att'y Gen. (May 18, 2023) https://www.atg.wa.gov/news/news-releases/ag-ferguson-s-lawsuit-forces-google-pay-nearly-40m-over-deceptive-location. [313] Press Release, Office of the Indiana Attorney General, *Attorney General Todd Rokita Secures $49.5 Million Multistate Settlement with Blackbaud for Data Breach* (Oct. 5, 2023), https://events.in.gov/event/attorney_general_todd_rokita_secures_495_million_multistate_settlement_with_blackbaud_for_data_breach. [314] Press Release, New York State Office of the Attorney General, *Attorney General James and Multistate Coalition Secure $6.5 Million from Morgan Stanley for Failing to Protect Customer Data* (Nov. 16, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-secure-65-million-morgan-stanley. [315] Press Release, New Jersey Office of the Attorney General, *AG Platkin Co-Leads $2.5-Million Multistate Settlement with EyeMed Over Data Breach that Compromised the Personal Information of Millions of Patients* (May 16, 2023), https://www.njoag.gov/ag-platkin-co-leads-2-5-million-multistate-settlement-with-eyemed-over-data-breach-that-compromised-the-personal-information-of-millions-of-patients/. [316] *See* Notice of Settlement and Joint Stipulation and [Proposed] Order to Stay Litigation Activities Pending Filing of Mot. for Prelim. Approval, *In re Orrick, Herrington & Sutcliffe, LLP Data Breach Litig.*, No. 3:23-cv-04089 (N.D. Cal. Dec. 21, 2023), ECF No. 50. [317] *See* Order Granting Final Approval of Class Action Settlement and Pls.' Mot. for Att'ys' Fees and Costs, *Desue v. 20/20 Eye Care Network Inc.*, No. 21-61275 (S.D. Fla. July 8, 2023), ECF No. 100. [318] Identity Theft Resource Center, *Q3 2023 Data Breach Analysis*, https://www.idtheftcenter.org/wp-content/uploads/2023/10/20231011_Q3-2023-Data-Breach-Analysis.pdf. [319] Identity Theft Resource Center, *Q3 2022 Data Breach Analysis*, https://www.idtheftcenter.org/wp-content/uploads/2022/10/20221005_One-Pager_Q3-2022-Data-Breach-Analysis.pdf. [320] *See* Transfer Order, *In re MOVEit Customer Data Sec. Breach Litig.*, MDL No. 3083 (J.P.M.L. Oct. 4, 2023); Judicial Panel on Multidistrict Litigation, *MDL Statistics Report – Distribution of Pending MDL Dockets by Actions Pending* (Jan. 2, 2014), https://www.jpml.uscourts.gov/sites/jpml/files/Pending_MDL_Dockets_By_Actions_Pending-January-2-2024.pdf. [321] *See In re MOVEit Customer Data Sec. Breach Litig.*, No. 23-3083 (D. Mass.). [322] *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021) (holding that plaintiffs who had not suffered concrete harm due to data breach, and instead claimed they are at heightened risk of future harm, lack standing to sue under Article III). [323] *Id.* at 437. [324] 72 F.4th 365, 375 (1st Cir. 2023) (holding that plaintiff adequately alleged standing based on the filing of a fraudulent tax return that likely resulted from information compromised in the data breach). [325] *Id.* at 377. [326] *Bohnak v. Marsh & McLennan Cos., Inc.*, 79 F.4th 276, 286 (2d Cir. 2023) (cleaned up). [327] *Id.* at 287. [328] 2023 WL 4183380, at *4 (E.D. Va. June 26, 2023). [329] *Id.* [330] *Id.* [331] *Id.* [332] *Id.* at *5. [333] 2023 WL 5608389, at *2 (C.D. Cal. Aug. 29, 2023) (acknowledging that while an increased risk of identity theft stemming from a data breach can constitute a threat of imminent harm sufficient for standing purposes, on the facts of the case, the username and password stolen in the breach were not linked to the plaintiff's financial accounts, and thus did not give rise to the threat of identity theft). [334] *Id.* [335] *See TransUnion*, 594 U.S. at 431 ("Every class member must have Article III standing in order to recover individual damages. Article III does not give federal courts the power to order relief to any uninjured plaintiff, class action or not."). [336] 344 F.R.D. 38, 52 (D.D.C. 2023). [337] *Id.* at 53. [338] *Id.* at 55. [339] *See* Cornerstone Research, *Securities Class Action Trend Cases*, https://www.cornerstone.com/insights/research/securities-class-action-trend-cases/. [340] Complaint ¶ 3, *Jaramillo v. Dish Networks Corp.*, No. 23-734 (D. Colo. Mar. 23, 2023), ECF No. 1. [341] Complaint ¶ 4, *Official Intel. Pty. Ltd., v. Block, Inc.*, No. 23-2789 (S.D.N.Y. April 3, 2023), ECF No. 1. [342] 15 U.S.C. § 78u-4(b)(2). [343] *In re Okta, Inc.*

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Securities Litig., 2023 WL 2749193, at *20 (N.D. Cal. Mar. 31, 2023). [344] *Id.* at *15. [345] *Id.* [346] *See, e.g.*, *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (9th Cir. May 31, 2022); *Popa v. Harriet Carter Gifts, Inc.*, 45 F.4th 687 (3d Cir. 2022). [347] 18 U.S.C. § 2510 *et seq.* [348] *Id.* § 2511(2)(d). [349] *See* Recording Law, *All Party (Two Party) Consent States – List and Details*, https://recordinglaw.com/party-two-party-consent-states/ (last visited Jan. 26, 2024) (identifying 13 two-party or all-party consent states). [350] *See, e.g.*, Cal. Penal Code §§ 631, 632 (wiretapping and eavesdropping statutes); *id.* § 637.2(a) (authorizing a private right of action and statutory damages). [351] *Doe v. Regents of Univ. of California*, No. 23-CV-00598-WHO, 2023 WL 3316766 (N.D. Cal. May 8, 2023). [352] *Jackson v. Fandom, Inc.*, No. 22-CV-04423-JST, 2023 WL 4670285 (N.D. Cal. July 20, 2023). [353] *Id.* at *4–5. [354] *Stark v. Patreon, Inc.*, 656 F. Supp. 3d 1018 (N.D. Cal. 2023). [355] *Id.* at 1039–40. [356] 18 U.S.C. § 1030(a). [357] *Van Buren v. United States*, 141 S. Ct. 1648, 1654–55 (2021). [358] Press Release, Department of Justice, *Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act* (May 19, 2022), https://www.justice.gov/opa/press-release/file/1507126/download. [359] *United States v. Calonge*, 74 F.4th 31, 36 (2d Cir. 2023), *cert. denied*, 2023 WL 7475309 (U.S. Nov. 13, 2023). [360] *Id*. at 33–34. [361] *Id*. at 33. [362] *Id*. at 33–34. [363] *Id*. at 35–36 (citing 18 U.S.C. § 1030(e)(8)). [364] *Calonge v. United States*, 2023 WL 7475309 (U.S. Nov. 13, 2023). [365] *ACW Flex Pack LLC v. Wrobel*, 2023 WL 4762596, at *6–7 (N.D. Ill. July 26, 2023). [366] *Id.* at *3, *6. [367] *Id.* at *5. [368] *Id*. at *6. [369] *Id.* (quoting 18 U.S.C. § 1030(e)(1)) (emphasis removed). [370] *Id.* at *6–8. [371] *Id.* at *7. [372] *iPurusa, LLC v. Bank of New York Mellon Corp.*, 2023 WL 3072686, at *7 (D.N.J. Apr. 25, 2023). [373] *Id.* at *6. [374] *Id.* at *7. [375] *Id.* [376] *See, e.g.*, *T. et al v. OpenAI LP et al.*, Case No. 23-cv-04557, Dkt. 1 ¶¶ 317–326 (N.D. Cal.); *P.M. et al v. OpenAI LP et al*., Case No. 23-cv-03199-TLT, Dkt. 1 ¶¶ 422–431 (N.D. Cal.); *see id.* Dkt. 38 (notice of voluntary dismissal). [377] *hiQ Labs, Inc. v. LinkedIn Corp*., 31 F.4th 1180 (9th Cir. 2022). [378] *Id.* at 1201. [379] Cal. Penal Code §§ 502(c)(2) & (e)(1). [380] *Id*. § 502(b)(1). [381] *Brown v. Google LLC*, 2023 WL 5029899, at *1 (N.D. Cal. Aug. 7, 2023). [382] *Id.* at *2. [383] *Id.* at *18. [384] *Id.* at *19 (citing Cal. Penal Code § 502(c)(2)). [385] *Id.* [386] *Brown et al. v. Google LLC*, Case No. 4:20-cv-03664, Dkt. 1089 (N.D. Cal.). [387] *Nora Gutierrez v. Converse Inc*., 2023 WL 8939221, at *1, *5 (C.D. Cal. Oct. 27, 2023). [388] *Id.* at *4 (quoting *In re iPhone Application Litig*., 2011 WL 4403963, at * 12 (N.D. Cal. Sept. 20, 2011)). [389] *Id.* [390] *Id.* at *5. [391] 47 U.S.C. § 227. [392] *Facebook, Inc. v. Duguid*, 592 U.S. 395 (2021). [393] *Dickson v. Direct Energy, LP*, 69 F.4th 338, 348–49 (6th Cir. 2023). [394] *Id*. at 345–48. [395] *Drazen v. Pinto*, 74 F.4th 1336, 1345–46 (11th Cir. 2023) (reversing *Salcedo v. Hanna*, 936 F.3d 1162, 1172 (11th Cir. 2019)). [396] *Hall v. Smosh Dot Com, Inc.*, 72 F.4th 983, 990–91 (9th Cir. 2023). [397] *Id.* at 990. [398] *Mauthe v. Millennium Health LLC*, 58 F.4th 93, 97 (3d Cir. 2023). The TCPA defines an "unsolicited advertisement" as "any material advertising the commercial availability or quality of any property, goods, or services which is transmitted to any person without that person's prior express invitation or permission, in writing or otherwise." 47 U.S.C. § 227(a)(5). [399] *Trim v. Reward Zone USA LLC*, 76 F.4th 1157, 1164 (9th Cir. 2023). [400] Cal. Civ. Code § 1798.150 (West 2023). [401] *California Consumer Privacy Act (CCPA) Litigation*, U.S. Cybersecurity and Data Privacy Outlook and Review - 2023 (Jan. 30, 2023), https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/. [402] Order Granting Final Approval of Class Action Settlement, *Service v. Volkswagen Grp. of Am., Inc.*, No. C22-01841 (Cal. Super. Ct. Contra Costa Cnty. May. 31, 2023), https://odyportal.cc-courts.org/Portal/DocumentViewer/DownloadDocumentFile/Download?d=10C938A76250CE4331774E2C729A0D43&c=EC610BADE930EF833C9117C84F5729FC&l=4C398088907DD05C6D76EE93BC04CDF4&cn=F44FB09A29DC4E11FE28DCC41D39CD99&fileName=C22-01841%20-%20Order%20Filed%20Re%20Granting%20Final%20Approval&docTypeId=3&isVersionId=False. [403] *Id.* at 4. [404] *Carter v. Vivendi Ticketing US LLC*, No. SACV2201981(DFMx), 2023 WL 8153712 (C.D. Cal. Oct. 30, 2023). [405] *Id.* [406] *Id.* at *2. [407] *Gershfeld v. Teamviewer US, Inc.*, No. SACV2100058(ADSx), 2021 WL 3046775 (C.D. Cal. June 24, 2021). [408] *Id.* at 2. [409] *Gershfeld v. TeamViewer US, Inc.*, No. 21-55753, 2023 WL 334015 (9th Cir. Jan. 20, 2023) (mem.). [410] *Alexander v. Wells Fargo Bank, N.A.*, No. 23-CV-617-DMS-BLM, 2023 WL 5109532 (S.D. Cal. Aug. 9, 2023). [411] *California Consumer Privacy Act*

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

(CCPA) Litigation, U.S. Cybersecurity and Data Privacy Outlook and Review - 2023 (Jan. 30, 2023), https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/. [412] *Brown v. Google LLC*, No. 4:20-CV-3664, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023). [413] *Id.* [414] *Id.* at *21. [415] *Id.* [416] *Id. at *21.* [417] *Id.* [418] Cal. Civ. Code § 1798.150(b). [419] *California Consumer Privacy Act (CCPA) Litigation*, U.S. Cybersecurity and Data Privacy Outlook and Review - 2023 (Jan. 30, 2023), https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/. [420] *Guy v. Convergent Outsourcing, Inc.*, No. C22-1558, 2023 WL 4637318 (W.D. Wash. July 20, 2023). [421] Cal. Civ. Code § 1798.150(b). [422] *Guy*, 2023 WL 4637318. [423] *Griffey v. Magellan Health Inc.*, No. CV-20-01282-PHX, 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022). [424] *Guy*, 2023 WL 4637318, at *9. [425] *Florence v. Order Express, Inc.*, No. 22 C 7210, 2023 WL 3602248 (N.D. Ill. May 23, 2023). [426] *Id.* at *7 (internal quotations omitted). [427] Cal. Civ. Code § 1798.150(b). [428] *Florence*, 2023 WL 3602248, at *7. [429] *California Consumer Privacy Act (CCPA) Litigation,* U.S. Cybersecurity and Data Privacy Outlook and Review - 2023 (Jan. 30, 2023), https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2023/. [430] *Durgan v. U-Haul Int'l Inc.*, No. CV-22-01565-PHX, 2023 WL 7114622 (D. Ariz. Oct. 27, 2023). [431] *Id.* at *7. [432] *Id.* at *6. [433] *In re Bank of Am. California Unemployment Benefits Litig.*, No. 21-MD-2992-LAB-MSB, 2023 WL 3668535 (S.D. Cal. May 25, 2023). [434] *Id.* at *13–15. [435] *Id.* at *15. [436] *Tims v. Black Horse Carriers, Inc.*, 216 N.E.3d 845 (Ill. 2023). [437] 735 Ill. Comp. Stat. Ann. 5/13-205 (2022). [438] *Tims*, 216 N.E.3d at 854. [439] *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918, 920 (Ill. 2023). [440] *Id.* at 928. [441] *Id.* at 929. [442] *Minor v. Oldcastle Servs. Inc.*, No. 21?CV?503?SMY (S.D. Ill. Mar. 22, 2023). [443] *Jones v. Microsoft Corp.*, No. 1:22?cv?03437 (N.D. Ill. Jan. 9, 2023). [444] *Id.* at 7–8. [445] *Warmack?Stillwell v. Christian Dior, Inc.*, No. 22?C?4633 (N.D. Ill. Feb. 10, 2023). [446] *Crumpton v. Octapharma Plasma, Inc.*, 513 F. Supp. 3d 1006, 1015–17 (N.D. Ill. 2021). [447] *Id.* [448] Tex. Bus. & Com. Code § 503.001. [449] *Tex. v. Meta Platforms, Inc.*, Cause No. 22-0121 (Tex. Dist. Ct. Feb. 8, 2023). [450] Press Release, Attorney General of Texas, *Paxton Sues Google for its Unauthorized Capture and Use of Biometric Data and Violation of Texans' Privacy* (Oct. 20, 2022), https://texasattorneygeneral.gov/news/releases/paxton-sues-google-its-unauthorized-capture-and-use-biometric-data-and-violation-texans-privacy. [451] *Gross v. Madison Square Garden Ent. Corp.*, No. 1:23-cv-03380 (S.D.N.Y. filed Apr. 21, 2023). [452] Second Amended Complaint at 2–3, *Gross v. Madison Square Garden Ent. Corp.*, No. 1:23-cv-03380 (S.D.N.Y. June 9, 2023). [453] *Id.* [454] *Id.* at 23–24. [455] *Id.* at 25. [456] Report & Recommendation, *Gross v. Madison Square Garden Ent. Corp.*, No. 23-cv-3380 (S.D.N.Y. Jan. 9, 2024). [457] *Id.* at 14. [458] *Id.* at 18. [459] *Id.* at 20 (quoting *Zoll v. Ruder Finn, Inc.*, No. 01-cv-139 (CSH), 2004 WL 42260, at *4 (S.D.N.Y. Jan. 7, 2004)). [460] *Id.* at 21. [461] *Id.* at 8–13. [462] 598 U.S. 471 (2023). [463] 598 U.S. 617 (2023). [464] *Taamneh*, 598 U.S. at 482. [465] *Gonzalez*, 598 U.S. at 621. [466] *Taamneh*, 598 U.S. at 501–02. [467] *Gonzalez*, 598 U.S. at 622. [468] *Minahan v. Google LLC*, No. 22-cv-5652, 2023 WL 3605329, at *1 (N.D. Cal. May 1, 2023), *appeal filed*, No. 23-15775 (9th Cir. May 22, 2023). [469] *Id.* at *2. [470] *M.K. v. Google LLC*, No. 21-cv-08465, 2023 WL 4937287 (N. D. Cal. filed Oct. 29, 2021). [471] *Id.* at *10. [472] *Id.* at *3. [473] *Id.* [474] *Id.* at *5. [475] *Id.* at *6–7. [476] *Ramirez v. The Paradies Shops, LLC*, 69 F.4th 1213, 1221 (11th Cir. 2023). [477] *Id.* at 1216. [478] *Id.* [479] *Id.* at 1220–21. [480] Class Action Complaint at 2–3, *Pai v. Tesla, Inc.*, Case 4:23-cv-04550 (N.D. Cal. filed Sept. 5, 2023). [481] *Id.* [482] *The Digital Revolution Engineering Smart City Infrastructure*, Utilities One (Oct. 27, 2023), https://utilitiesone.com/the-digital-revolution-engineering-smart-city-infrastructure. [483] Ashley Johnson, *Balancing Privacy and Innovation in Smart Cities and Communities*, Info. Tech. & Innovation Found. (Mar. 6, 2023), https://itif.org/publications/2023/03/06/balancing-privacy-and-innovation-in-smart-cities-and-communities/. [484] *Id.* [485] Diana Baker Freeman, *Why Local Governments Are a Target for Cyber Attacks and Steps to Prevent It*, Governing (May 6, 2022), https://www.governing.com/sponsored/why-local-governments-are-a-target-for-cyber-attacks-and-steps-to-prevent-it. [486] Richard Forno, *Local Governments Are Attractive Targets for Hackers and Are Ill-Prepared*, Ctr. for Internet & Soc'y (Mar.
28,

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

2022), https://cyberlaw.stanford.edu/blog/2022/03/local-governments-are-attractive-targets-hackers-and-are-ill-prepared. [487] Ashley Johnson, *Balancing Privacy and Innovation in Smart Cities and Communities*, Info. Tech. & Innovation Found. (Mar. 6, 2023), https://itif.org/publications/2023/03/06/balancing-privacy-and-innovation-in-smart-cities-and-communities/. [488] *Id.* [489] Maya Shwayder, *The Future of Smart Cities May Mean the Death of Privacy*, Digit. Trends (Apr. 22, 2020), https://www.digitaltrends.com/news/smart-cities-privacy-security/. [490] Ashley Johnson, Balancing Privacy and Innovation in Smart Cities and Communities, Info. Tech. & Innovation Found. (Mar. 6, 2023), https://itif.org/publications/2023/03/06/balancing-privacy-and-innovation-in-smart-cities-and-communities/. [491] *What is Edge Computing?*, IBM (last visited Jan. 18, 2024), https://www.ibm.com/topics/edge-computing. [492] Mary K. Pratt, *7 Edge Computing Trends to Watch in 2023 and Beyond*, TechTarget (Dec. 8, 2022), https://www.techtarget.com/searchcio/tip/Top-edge-computing-trends-to-watch-in-2020. [493] *Id.* [494] *Id.* [495] *Id.* [496] Pete Swabey, *Why Edge Computing is a Double-Edged Sword for Privacy*, Tech Monitor (Mar. 31, 2023), https://techmonitor.ai/focus/privacy-on-the-edge-why-edge-computing-is-a-double-edged-sword-for-privacy. [497] *Id.* [498] *Id.* [499] *Id.* [500] Matthew Gooding, *Can GAIA-X Solve Europe's Data Sovereignty Problem?*, Tech Monitor (Apr. 8, 2021), https://techmonitor.ai/technology/cloud/what-is-gaia-x-eu-data-sovereignty. [501] Executive Office of the President, Office of Science and Technology Policy, *National Strategy To Advance Privacy-Preserving Data Sharing and Analytics* (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf. [502] OECD, *Emerging Privacy-Enhancing Technologies, Current Regulatory and Policy Approaches*, OECD Digital Economy Papers, No. 351, 2 (Mar. 2023), https://www.oecd-ilibrary.org/deliver/bf121be4-en.pdf?itemId=/content/paper/bf121be4-en&mimeType=pdf. [503]Executive Office of the President, Office of Science and Technology Policy, *National Strategy To Advance Privacy-Preserving Data Sharing and Analytics* (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf. [504] *Id.* [505] *Id.* [506] *Id.* [507] *Id.* [508] *Id.* [509] *Id.* [510] *Id.* [511] Pete Swabey, *Why Edge Computing is a Double-Edged Sword for Privacy*, Tech Monitor (Mar. 31, 2023), https://techmonitor.ai/focus/privacy-on-the-edge-why-edge-computing-is-a-double-edged-sword-for-privacy. [512] Executive Office of the President, Office of Science and Technology Policy, *National Strategy To Advance Privacy-Preserving Data Sharing and Analytics* (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf. [513] *Id.* [514] Shafi Goldwasser et al., *The Knowledge Complexity of Interactive Proof Systems*, 18 SIAM J. Computing 186 (1989). [515] Eli Ben-Sasson et al., *Zerocash: Decentralized Anonymous Payments from Bitcoin*, Zerocash, (May 18, 2014), http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf. [516] Tianyi Liu et al., *zkCNN: Zero Knowledge Proofs for Convolutional Neural Network Predictions and Accuracy*, Comput. & Commc'ns Sec. (2021), https://doi.org/10.1145/3460120.3485379. [517] Executive Office of the President, Office of Science and Technology Policy, *National Strategy To Advance Privacy-Preserving Data Sharing and Analytics* (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf. [518] *Id.* [519] *Id.* [520] Jennifer Bryant, *European Commission Adopts EU-US Adequacy Decision*, Int'l Ass'n Priv. Pros. (July 10, 2023), https://iapp.org/news/a/european-commission-adopts-eu-u-s-adequacy-decision/. [521] *Id.* [522] Natasha Lomas, *Europe's Top Court Strikes Down Flagship EU-US Data Transfer Mechanism*, TechCrunch (July 16, 2020), https://techcrunch.com/2020/07/16/europes-top-court-strikes-down-flagship-eu-us-data-transfer-mechanism/. [523] Natasha Lomas, *Europe Adopts US Data Adequacy Decision*, TechCrunch (July 10, 2023), https://techcrunch.com/2023/07/10/eu-us-data-privacy-framework-adoption/. [524] *Id.* [525] *Id.* [526] Press Release, Department of Commerce, *Data Privacy Framework Program Launches New Website Enabling U.S. Companies to Participate in Cross-Border Data Transfers* (July 17, 2023), https://www.commerce.gov/news/press-releases/2023/07/data-privacy-framework-

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

program-launches-new-website-enabling-us. [527] Press Release, Senator Ron Wyden, *Wyden, Lee, Davidson and Lofgren Introduce Bipartisan Legislation to Reauthorize and Reform Key Surveillance Law, Secure Protections for Americans' Rights* (Nov. 7, 2023), https://www.wyden.senate.gov/news/press-releases/wyden-lee-davidson-and-lofgren-introduce-bipartisan-legislation-to-reauthorize-and-reform-key-surveillance-law-secure-protections-for-americans-rights. [528] Noah Chauvin & Elizabeth Goitein, *Reform Bill Would Protect Americans from Warrantless Surveillance*, Brennan Ctr. for Just. (Nov. 7, 2023), https://www.brennancenter.org/our-work/analysis-opinion/reform-bill-would-protect-americans-warrantless-surveillance. [529] On December 22, 2023, President Biden signed the National Defense Authorization Act, which included a Congressional measure extending Section 702 until mid-April 2024. Rebecca Beitsch, *Congress Approves Short-Term Extension of Warrantless Surveillance Powers*, The Hill (Dec. 12, 2023), https://thehill.com/policy/national-security/4360341-fisa-congress-approves-short-term-extension-warrantless-surveillance-powers; *see also* Press Release, White House, *Joseph R. Biden, Statement from President Biden on H.R. 2670, National Defense Authorization Act for Fiscal Year 2024* (Dec. 22, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/22/statement-from-president-joe-biden-on-h-r-2670-national-defense-authorization-act-for-fiscal-year-2024/. [530] Noah Chauvin & Elizabeth Goitein, *Reform Bill Would Protect Americans from Warrantless Surveillance*, Brennan Ctr. for Just., (Nov. 7, 2023), https://www.brennancenter.org/our-work/analysis-opinion/reform-bill-would-protect-americans-warrantless-surveillance. [531] *Id.* [532] *Id.* [533] *Id.* [534] *Id.* [535] *Electronic Communications Privacy Act (ECPA)*, Elec. Priv. Info. Ctr. (last visited Jan. 19, 2024), https://epic.org/ecpa/; *see also* Press Release, Senator Ron Wyden, *Wyden, Lee, Davidson and Lofgren Introduce Bipartisan Legislation to Reauthorize and Reform Key Surveillance Law, Secure Protections for Americans' Rights* (Nov. 7, 2023), https://www.wyden.senate.gov/news/press-releases/wyden-lee-davidson-and-lofgren-introduce-bipartisan-legislation-to-reauthorize-and-reform-key-surveillance-law-secure-protections-for-americans-rights. [536] Government Surveillance Reform Act of 2023, S. 3234, 118th Cong. (2023). [537] *Id.* § 504. [538] *Id.*; 47 U.S.C. § 230(f) (2000). [539] Government Surveillance Reform Act of 2023, S. 3234, 118th Cong. § 504 (2023). [540] *Id.* § 501–11. [541] *Id.* [542] *Id.* § 508. [543] *Id.* § 503. [544] India McKinney, *The House Intelligence Committee's Surveillance 'Reform' Bill is a Farce*, Elec. Frontier Found. (Dec. 8, 2023), https://www.eff.org/deeplinks/2023/12/section-702-needs-reform-and-oversight-not-expansion-congress-should-oppose-hpsci; *see also* Jules Roscoe, *Congress Pulls Bill That Would Massively Expand Surveillance After 'Dramatic Showdown'*, Vice (Dec. 12, 2023), https://www.vice.com/en/article/y3wkdg/fisa-surveillance-bill-congress-pulled. [545] Jules Roscoe, *Congress Pulls Bill That Would Massively Expand Surveillance After 'Dramatic Showdown'*, Vice (Dec. 12, 2023), https://www.vice.com/en/article/y3wkdg/fisa-surveillance-bill-congress-pulled. [546] *Id.* [547] Press Release, ACLU, *Ahead of House Vote, ACLU Sounds Alarm on Bill Greatly Expanding the Government's Mass Warrantless Surveillance Authority* (Dec. 11, 2023), https://www.aclu.org/press-releases/ahead-of-house-vote-aclu-sounds-alarm-on-bill-greatly-expanding-the-governments-mass-warrantless-surveillance-authority.

The following Gibson Dunn lawyers assisted in preparing this alert: Alexander Southwell, Cassandra Gaedt-Sheckter, Natalie Hausknecht, Martie Kutscher Clark, Timothy Loose, Abbey Barrera, Jacob Arber, Tony Bedel, Matt Buongiorno, Eric Hornbeck, Jay Mitchell*, Wesley Sze, Terry Wong, Najatt Ajarar, Michael Brandon, Tawkir Chowdhury, Lanie Corrigan, Justine Deitz, Skylar Drefcinski, Sasha Dudding, Kunal Kanodia, Erin Kim, Brendan Krimsky, Ruby Lang, Emma Li, Ignacio Martinez Castellanos, Jay Minga, Peter Moon, Narayan Narasimhan*, Mason Pazhwak, Matthew Reagan, John Ryan, Christopher Scott*, Becca Smith, Snezhana Stadnik Tapia, Graham Miller Stinnett, Cydney Swain, Julie Sweeney, Trenton Van Oss, Hayato Watanabe, Diego Wright, and Samantha Yi*.

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 leader or member of the firm's Privacy, Cybersecurity & Data Innovation practice group: **United States**: S. Ashlie Beringer – Co-Chair, Palo Alto (+1

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

650.849.5327, aberinger@gibsondunn.com) Jane C. Horvath – Co-Chair, Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com) Ryan T. Bergsieker – Denver (+1 303.298.5774, rbergsieker@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) 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) Alexander H. Southwell – New York (+1 212.351.3981, asouthwell@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) Debra Wong Yang – Los Angeles (+1 213.229.7472, dwongyang@gibsondunn.com) **Europe**: Ahmed Baladi – Co-Chair, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com) Nicholas Banasevic* – Managing Director, Brussels (+32 2 554 72 40, banasevic@gibsondunn.com) Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com) Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com) Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com) Lars Petersen – Frankfurt/Riyadh (+49 69 247 411 525, lpetersen@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) **Nicholas Banasevic, Managing Director in the firm's Brussels office and an economist by background, is not admitted to practice law. *Jay Mitchell and Samantha Yi are associates in the Washington, D.C. office. Jay is admitted in California and Illinois, and Samantha is admitted in Maryland; both are practicing under supervision of members of the District of Columbia Bar under D.C. App. R. 49. *Narayan Narasimhan and Christopher Scott, recent law graduates in the New York office, are not admitted to practice law.* © 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

Privacy, Cybersecurity, and Data Innovation

© 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**