Legal 500
Country Comparative Guides 2024

United States

Data Protection & Cybersecurity

Contributor

Orrick, Herrington & Sutcliffe LLP

Heather Egan

Partner | hegan@orrick.com

Sulina Gabale

Partner | sgabale@orrick.com

Thora Johnson

Partner | thora.johnson@orrick.com

Emily S. Tabatabai

Partner | etabatabai@orrick.com

Shannon Yavorsky

Partner | syavorsky@orrick.com

Bianca Giulia Ponziani

Managing Associate | bponziani@orrick.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in United States.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

United States: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

There is no single, omnibus U.S. federal law addressing privacy and cybersecurity rights and obligations. Federal laws, which apply to residents in all states, are generally sector-specific and primarily regulate the financial and health care sectors, the telecom industry, government contractors and children. Under the U.S. system, states may regulate absent federal preemption or an undue burden on interstate commerce. Accordingly, an increasing number of states have passed comprehensive privacy laws, in addition to state sector-specific data protection laws, applicable to residents of that state or data processing activity taking place in the state.

At the federal level, key laws include the Gramm-Leach-Bliley Act ("GLBA"), which protects personal information held by financial institutions and related companies collected as part of the provision of financial services; the Fair Credit Reporting Act ("FCRA"), which regulates use of information to make employment, credit, insurance or certain other determinations; the Privacy Act of 1974 and the Federal Information Security Management Act of 2002 ("FISMA"), which regulate use of personal information by the government and government contractors; the Health Insurance Portability and Accountability Act ("HIPAA"), which regulates information related to health status that can be linked to an individual under the control of certain covered entities and their contractors and regulates the collection, disclosure and security of such information; the Cable Communications Privacy Act of 1984 ("Cable Act"), Video Privacy Protection Act ("VPPA"), Electronic Communications Privacy Act ("ECPA") and Stored Communications Act ("SCA"), which protect the privacy of certain types of communications and content; the Children's Online Privacy Protection Act ("COPPA"), which regulates personal information collected online from children under the age of 13 and requires related privacy notices and, in many instances, verified parental consent; the Family Educational Rights and Privacy Act ("FERPA"), which protects the privacy of educational records; and the Cybersecurity Information Sharing Act, which encourages private companies to share information about cyber threats with the government and provides liability protections for companies that do.

Moreover, federal laws, such as the Telephone Consumer Protection Act ("TCPA") and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the "CAN-SPAM Act"), also regulate calling or texting phone numbers for both marketing and nonmarketing purposes and the sending of email messages, respectively. Depending on the law, federal privacy laws are primarily enforced by the Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau ("CFPB"), the Department of Health & Human Services ("HHS"), or the Office of the Comptroller of the Currency ("OCC"). The FTC is the principal regulator of consumer privacy under its authority to regulate deceptive or unfair practices in or affecting commerce, require companies to disclose unexpected data practices prior to collection, enforce failures to comply with published privacy policies, and require companies to reasonably protect personal information in their custody or under their control. However, State Attorneys General often have enforcement authority under many Federal privacy laws as well as under the States' own unfair and deceptive trade practices acts.

Many states also have data protection laws that protect the personal information of residents, but the level of protection and the types of information considered to be "personally identifiable" differ from state to state.

Some states are more protective of privacy than others. Massachusetts, for example, has data security laws requiring comprehensive data security planning for any entity obtaining or storing personal information. New York has similar regulations requiring comprehensive cybersecurity planning for businesses that own or license private information of New York residents, as well as financial institutions doing business in New York. The New York Department of Financial Services ("NYDFS") Cybersecurity Regulation (23 NYCRR 500) applies to all entities regulated under NYDFS and by extension, unregulated third-party service providers of regulated entities, and imposes cybersecurity requirements on all covered entities and applicable third parties. Illinois, Washington and Texas have enacted biometric privacy laws imposing special protections for biometric data, such as [INSERT] that can be used to identify a unique

individual. California, Vermont, Texas and Oregon recently enacted laws that impose additional privacy and data protection requirements on "data brokers" (companies which sell data they did not collect directly from the data subject), including registration. In addition, the data broker laws in Vermont and Texas (effective Jan 1, 2024) require data brokers to implement and maintain robust information security programs that include a number of enumerated physical, administrative and technical safeguards.

Among the states, California has been especially protective of consumer privacy. Historically, California offered limited protections under California's Shine the Light law and the California Online Privacy Protection Act ("CalOPPA"), which were copied in large part by Nevada and Delaware. California became the first U.S. state to pass a comprehensive consumer privacy law, the California Consumer Privacy Act ("CCPA"), which took effect January 1, 2020. The CCPA imposed European-style data subject rights of data access and portability, data deletion and the right to opt-out of personal information "sales", defined broadly to mean "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or third party for monetary or other valuable consideration." The CCPA also requires relatively granular disclosures in privacy notices and the right of California consumers to obtain very specific information on a business's practices regarding their own personal information upon verified request. In addition, companies may not discriminate against California consumers who exercise their CCPA rights. The California Privacy Rights Act ("CPRA"), passed by a majority vote in the November 2020 statewide election, substantially amends and amplifies the requirements of the CCPA, addressing ambiguities and overly burdensome requirements, while simultaneously introducing new privacy and security obligations for covered businesses. For example, the CPRA revises and expands the scope of covered "businesses" under the CCPA, adds a second category of personal information ("sensitive personal information"), broadens the notice at collection requirements, adopts an explicit overarching purpose-limitation obligation, and adds new consumer rights and revises existing obligations. The CPRA became fully operative on January 1, 2023. Corresponding updates were made to the CCPA's implementing regulations, which took effect March 29, 2023. Further rulemaking relating to automated decision-making, cybersecurity audits, and risk assessments are expected to be finalized in 2024.

Following California, more than a dozen other U.S. states enacted comprehensive consumer data protection legislation: the Virginia Consumer Data Protection Act ("VCDPA") came into effect on January 1, 2023; the Colorado Privacy Act ("CPA") and the Connecticut Data Privacy Act ("CTDPA") came into effect on July 1, 2023; the Utah Consumer Privacy Act ("UCPA") came into effect on December 31, 2023; the Oregon Consumer Privacy Act ("OCPA"), Florida Digital Bill of Rights ("FDBR"), and Texas Data Privacy and Security Act ("TDPSA") will come into effect on July 1, 2024; the Montana Consumer Data Privacy Act ("MCDPA") will come into effect on October 1, 2024; the Iowa Consumer Data Protection Act ("ICDPA") and Delaware Personal Data Privacy Act ("DPDPA") and the New Hampshire Privacy Act ("NHPA") will come into effect on January 1, 2025; the New Jersey Data Privacy Act ("NJDPA") will come into effect on January 15, 2025; the Tennessee Information Protection Act ("TIPA") will come into effect on July 1, 2025; and the Indiana Consumer Data Protection Act ("INCDPA") will come into effect on January 1, 2026. While there is some variation between and among these state laws, they are generally similar to the CCPA, and impose data protection obligations on both controllers and processors establish consumer rights (*e.g.*, right to request access, correction, deletion) as well as the opt in/out of certain activities, such as data sales, targeted advertising, profiling or automated decision making, and the processing of sensitive personal information, among other obligations. To varying extents, these laws also enshrine the principles of data minimization, purpose limitation, enhanced transparency and consumer choice, and limits on data retention or secondary use.

Older state laws require specific privacy disclosures and/or restrict the collection of any or certain personal information in connection with credit card or other commercial transactions, except as necessary to complete the transaction. Several states also have privacy and data protection laws specific to the insurance industry that impose greater obligations on licensed insurance businesses than those mandated by the GLBA. States have also passed laws protecting employee privacy, including the privacy of their social media accounts and activities, and in other cases provide greater levels of student privacy than are accorded under FERPA. Around a dozen states have their own, often more restrictive version, of the VPPA.

All states have data security and breach notification laws, though the scope of what data is covered, as well as the corresponding notice and reporting obligations, vary from state to state.

Due to the patchwork nature of U.S. federal and state

privacy laws, the best course of action is to consult with skilled legal counsel to advise on a particular situation.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

Notably, several comprehensive state privacy laws listed above will come into effect later this year, including the OCPA and TDPSA (July 1, 2024) and the MCDPA (October 1, 2024). Further guidance regarding state privacy law obligations currently in effect are still pending, and additional implementing regulations and official guidance interpreting these new state laws will continue to be updated, proposed, developed and published in the coming year.

Currently, nearly two dozen other states are considering comprehensive privacy legislation. This increased momentum for comprehensive privacy bills at the state level will likely continue throughout 2024 and beyond. In addition, the federal government and several states are considering narrowly-scoped bills focused on children's personal data, biometrics, health data and artificial intelligence, as further detailed below.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

The United States does not have any privacy and cybersecurity-oriented general requirements to register personal information processing activities. However, certain industry-specific self-regulatory programs that touch on privacy may be applicable. For example, institutions that require a license from the NYDFS must certify annually that their organizations are in compliance with 23 NYCRR 500. The Payment Card Industry Data Security Standard (PCI DSS)—a standard enforced by contract, not law—provides security requirements for all entities accepting or processing payment transactions and might apply in this scenario. The digital advertising industry is governed by self-regulatory principles enforced by the Digital Advertising Alliance (DAA) and the Network Advertising Initiative (NAI). The DAA has developed and enforces privacy practices for digital advertising, providing consumers with enhanced transparency. To use the DAA's advertising option icon, however, requires a license. The NAI has established and enforces self-regulatory standards among its members.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

Because there is no single, overarching privacy law in the United States, there is no single concept of personal data or personal information. In general, all U.S. privacy laws protect some form of "personal data," "personal information" or "personally identifiable information", but the scope of coverage varies significantly. Personal data generally means any data or information that is linked to or reasonably related to an identified or identifiable individual, including name, date of birth, mailing address, and email address, as well as persistent identifiers that can be linked to a particular computer or device. Most U.S. state consumer privacy laws have special provisions addressing sensitive personal data, which generally means personal data revealing racial or ethnic original, political opinions, religious or philosophical beliefs, or genetic data, biometric data, or data concerning mental or physical health. These laws often require additional disclosures or safeguards before such sensitive personal data can be collected or processed.

The definition of "personal data" under U.S. state consumer privacy laws also varies. The CCPA defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," and excludes de-identified data and publicly available information. The CCPA cites as examples of personal information: unique ID, IP address, device ID and usage data; demographics and classifications; transactions and inquiries; biometric information; geolocation data; audio, electronic, visual, thermal, olfactory or similar information; preferences; inferences drawn to create a profile about a consumer; and educational information. These data elements fall into the CCPA's 11 categories of personal information, which must be referenced in related CCPA disclosures. The CCPA also creates a subset of "sensitive personal information" that carries additional compliance requirements, described further below. Under the CCPA, the definition of sensitive personal information includes, among other data elements, personal information that

reveals a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; personal information that reveals the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; precise geolocation; biometric data; and personal information collected and analyzed concerning a consumer's health. Other U.S. state privacy laws such as the VCDPA, CPA, CTDPA, UCPA, and ICDPA set forth similar definitions of "personal data" and "sensitive data."

For personal data breach notification purposes, the definition of "personal data" (or such equivalent term) is usually set out in each state's personal data breach notification law. Most personal data breach notification laws define personal information as an individual's name, plus:

- Social Security number;
- driver's license number or other government-issued identifier; or
- credit card number, bank account number or financial account number, if paired with sufficient information to access the account.

Increasingly, states are amending their personal data breach notification laws to add medical information or health insurance number and username and password to the definition of "personal data". Any breach involving the unauthorized access or acquisition of this information would require notification to the individual to whom the data relates.

Other definitions of "personal data" or such equivalent terms under federal U.S. law include:

- personal information of children under 13, as defined under COPPA;
- "protected health information" or "PHI," as defined under HIPAA; "nonpublic personal information," as defined under the GLBA; and
- "consumer credit and other information," as defined under the FCRA.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

Privacy laws in the United States generally do not include express principles related to the processing of personal information. Accordingly, there is no uniform view of how personal information should be processed in all contexts. That said, however, similar to the Fair Information Practice Principles issued by the Organization for Economic Cooperation and Development ("OECD"), the FTC has promulgated fair information practice principles ("FIPPs") as guidelines for the way in which online entities collect, process, and safeguard personal data to help ensure that the data processing practices are fair and provide adequate information security. The "core" FIPPs are: (i) notice / awareness; (ii) choice / consent; (iii) access / participation; (iv) integrity / security; and (v) enforcement / redress. The latter principle, enforcement / redress, was removed in the FTC's 2000 report to Congress.

i. The notice principle requires consumers to be made aware of an entity's data practices prior to such entity's collection of their personal data. Without providing prior notice, informed consent to such collection cannot be given. Three of the other FIPPs (choice/consent, access/participation, and enforcement/redress) are meaningful only upon notice to a consumer of an entity's data handling practices and the consumer's rights with respect to their personal data.
ii. The choice/consent principle refers to consumer choice or consent—that is, providing a consumer options as to whether their personal data is collected, how it is used, and whether any secondary uses of information are permitted (i.e., uses beyond those to which they consented or that are necessary to complete the contemplated transaction).
iii. The access/participation principle relates to a consumer's ability to view the personal data that an entity has collected, used, or disclosed about them, and to timely correct inaccurate or incomplete data the entity may hold about them. Under this principle, businesses should make available an inexpensive mechanism by which consumers may access or correct their personal data.
iv. The integrity/security principle requires entities to take reasonable steps to ensure that the personal data they process about a consumer is accurate and secure, such as using reputable data sources and providing the consumer access to their data for validation purposes.
v. The enforcement/redress principle relates to the various means by which FIPPs may be enforced and thus effective: self-regulation by

information collects; private rights of action; and government enforcement (*g.*, through civil and criminal penalties). Absent an enforcement or redress mechanism, the incentive for an entity to institute and comply with policies and procedures that align with the FIPPs is likely to be lost.

Currently, the FIPPs are not enforceable by law: they are only consumer-friendly data processing recommendations. The enforcement of and adherence to these principles is mainly accomplished through self-regulation, if at all. The FTC has, however, made efforts to monitor industry self-regulation, provided guidance for developing information practices, and has used its authority under the FTC Act to enforce promises made by businesses in their external privacy notices.

The FIPPs themselves underlie both federal and state laws and continue to serve as a model for data protection in developing areas and industries. For example, in California, the CCPA codifies a key FIPP concept by imposing an explicit, overarching purpose limitation principle requiring a business to collect, use, retain and share a consumer's personal information only as "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected." Likewise, the VCDPA imposes both a collection and purpose limitation requiring controllers to obtain consumer consent for processing personal data for a purpose neither reasonably necessary nor compatible with the disclosed purposes for which the personal data was collected. The CPA also creates several specific processing duties for controllers, including transparency, purpose specification, data minimization, avoiding secondary uses, a duty of care, avoiding unlawful discrimination, and the protection of sensitive data.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

No single federal U.S. law in sets out general requirements for when and how a controller must obtain consent from consumers: instead, consent requirements are regulated by various U.S. state and sector specific laws. To be sure, in the United States, the collection of certain categories of personal data requires opt-in consent, including the collection of health information, credit reports, financial information, student and children's data, biometric data, information about video viewing choices, certain uses of phone numbers, and geolocation data. Certain other uses of personal data are subject to opt-out consent, including email marketing under the CAN-SPAM Act or the "sale" of personal data under the CCPA. Still, certain other categories of personal data are subject to no consent requirement at all.

Federal U.S. law regulates the type of consent that a controller must obtain prior to communicating with an individual directly via telephone, text message, or fax. For example, under the TCPA, in many circumstances consent must be obtained from the recipient of a marketing telephone call or text message before the call is placed or the text message is sent. Whether and what kind of consent (no consent, "prior express consent," "prior express written consent") depends on the type of call (emergency, marketing, transactional); the type of calling technology (manual dial, auto-dialer, prerecorded voice); the recipient's line (residential landline, cell phone); the type of caller (for-profit entity, nonprofit, state or local government, federal government); and the category of recipient (business-to-consumer, business-to-business). In addition, under the FTC Act, controllers must generally obtain opt-in consent prior to using, disclosing or otherwise processing personal data in a manner that materially differs from the controller's privacy notice applicable at collection.

Certain states require controllers to obtain specific types of consent prior to collection, depending on the category of personal data at issue. As a notable example, the Illinois Biometric Information Privacy Act ("BIPA") requires that written consent be obtained before collecting a biometric identifier.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

The required form, content, and administration of a consent is determined by the law governing collection of the underlying personal data, taking into account the purposes for which personal data was collected (*e.g.*, marketing versus non-marketing purposes) and the type(s) of data collected (*e.g.*, sensitive data versus non-sensitive data). Generally, consent should be informed, freely given, unambiguous, and specific.

Both states and the FTC have been increasingly focused on prohibiting "dark patterns," namely user interfaces that

are designed or manipulated with the substantial effect of subverting or impairing autonomy, decision-making or choice. For example, both the CCPA and the CPA specify that consumer consent is not valid if obtained through a dark pattern. Likewise, the FTC published a 2022 report, "*Bringing Dark Patterns to Light*," which identifies common dark pattern tactics and issues recommendations to help avoid design practices that could be considered dark patterns.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

While there is no uniform legal approach in the United States to the processing of sensitive personal data, certain categories of data associated with sensitive personal data (financial data, health data, student, and children's data) are commonly subject to heightened protections. For example, HIPAA imposes privacy and security obligations on entities that handle protected health information; the GLBA protects "nonpublic personal information" that financial institutions maintain; the FCRA governs how consumer reporting agencies may collect, use, and disclose consumer credit information; and the Genetic Information Nondiscrimination Act prohibits certain uses of genetic information. Certain state laws also govern the processing of sensitive personal: Illinois' BIPA regulates the collection, use, and retention of biometric information, and the NYDFS Cybersecurity Regulation imposes heightened security safeguards for regulated financial institutions and insurers. The New York SHIELD Act also differentiates between "personal information" and "private information," with private information being a subset of personal data that is arguable more "sensitive," including, among other data elements, biometric information and account details that would allow for access to an individual's financial account. Relatedly, certain federal and state nondiscrimination laws prohibit the solicitation of certain types of personal data or using such data to the detriment of a protected class or group, particularly in the housing, employment, and credit contexts. California's Unruh Civil Rights Act prohibits discrimination in public accommodations, or the offering of products or services based on any of a number of protected classes or any other arbitrary classification. Protected groups, depending on the law at issue, include those discriminated against on the basis of sex, gender, religion, age, race, ethnicity, citizenship, ideology, political affiliation, creed, appearance, family status, sexual orientation, health status, military or veteran status, or source of income.

Several U.S. state privacy laws also require specific disclosures for the collection of sensitive personal data. For example, the CCPA requires covered businesses to disclose the purposes for which sensitive personal data may be collected and whether they sell or share sensitive personal data. Without first providing the consumer with notice, the CCPA also prohibits businesses from collecting additional categories of sensitive personal data or using sensitive personal data for purposes incompatible with the purpose for which it was collected. The CPRA also introduced the right to limit use and disclosure of sensitive personal information, which, absent an exception, requires businesses to publish a "Limit the Use of My Sensitive Personal Information" link (or equivalent) on its digital properties. Similarly, under the VCDPA and CPA, controllers are prohibited from processing sensitive personal data without first obtaining consumer consent. The UCPA will prohibit controllers from processing sensitive data without first presenting consumers with clear notice and the opportunity to opt-out of such processing.

9. How do the data protection laws in your jurisdiction address health data?

HIPAA and its implementing regulations established the first set of national U.S. standards for the broad protection of individually identifiable health information (Title 42 of the Code of Federal Regulations Part 2: Confidentiality of Substance Use Disorder Patient Records was first promulgated in 1975, but was federal law of a more limited scope, addressing only the confidentiality of substance use disorder information). HIPAA applies only to protected health information in the hands of covered entities and business associates. Covered entities are health plans, health care clearinghouses, and health care providers that engage in certain electronic transactions. Most, but not every, health care provider is subject to HIPAA. Business associates perform certain functions that involve the use or disclosure of protected health information for or on behalf of covered entities. HIPAA requires covered entities to designate a privacy officer and a security officer and requires business associates to designate a security officer (though, in practice, business associates also appoint a privacy officer to help oversee the HIPAA privacy program).

The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits on disclosures of PHI without authorization. The HIPAA Security Rule requires the use of

administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of electronic protected health information. Although there are no HIPAA retention requirements for medical records, HIPAA provides that covered entities must maintain a record of any policies, procedures, actions, or assessment carried out pursuant to HIPAA for a minimum of six years after their creation or six years from when a policy was last in effect. The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, HHS, and for large breaches, the media, of a breach of protected health information.

And while this federal standard established a floor, states are permitted to establish more stringent standards to govern health information. In fact, many have enacted laws that govern the confidentiality, use, and disclosure of medical records. For example, California's Confidentiality of Medical Information Act ("CMIA"), which is similar to HIPAA, protects the privacy of individually identifiable medical information obtained by a health care provider from a patient. The law applies to most health care providers and limits the circumstances in which medical information can be used or disclosed. In general, health care providers are prohibited from disclosing a patient's medical information without first obtaining the patient's written consent, subject to several limited exceptions.

As described above, the various comprehensive consumer data protection laws also provide special protections for health data as sensitive personal data. These laws differ in how inclusive they are, with some protecting physical and mental health conditions and others only protecting physical and mental health diagnoses.

On March 31, 2024, two new U.S. state privacy laws regulating consumer health data took effect: Washington's My Health My Data Act ("MHMD Act") and Nevada's similar law (SB 370). While excepting PHI under HIPAA, these statutes take a broad view of what constitutes consumer health data, capturing information about "bodily functions," "measurements," and biometrics. This has the effect of potentially bringing under their ambit of the laws businesses that do not squarely operate in the healthcare space (*e.g.*, food delivery services that collect information about consumer dietary preferences). Neither law is limited to residents of the applicable state, but also consumers whose health data is processed in either state. Among other obligations, these state consumer health data laws require covered businesses to post a consumer health data privacy notice on their Internet homepage and any page where consumer health data is collected; obtain consumer consent to collect and disclose health information where not necessary to the services provided; enter into data processing agreements with processors of consumer health data; and provide individual rights of access, withdrawal of consent, and deletion with respect to consumer health data collected about consumers. The Washington Attorney General has authority to bring enforcement actions under the MHMD Act, and unlike Nevada's similar law, consumers have a private right of action. Nevada's Attorney General may seek injunctive relief and monetary damages for violations.

Moreover, amendments to the CTDPA have also come into effect, including those related to consumer health data privacy protections. Unlike the MHMD Act and Nevada's similar law, the CTDPA limits the definition of "consumer" to just Connecticut residents. While CTDPA also takes a broad view of what constitutes consumer health data, though the definition is narrower than the MHMD Act and Nevada's similar law; notably, the CTDPA includes consumer health data in its definition of "sensitive data" (to be sure, as do a number of other state privacy laws), which requires controllers to conduct data protection assessments for relevant activities and to obtain consumer consent prior to collecting consumer health data. The CTDPA will be enforced by the Connecticut Attorney General and includes no private right of action.

The introduction of laws governing the processing of consumer health data in Washington, Nevada, and Connecticut have led to the emergence of a new industry term, with many practitioners collectively identifying these laws as "U.S. state consumer health privacy laws."

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Generally, U.S. federal and state privacy laws include a number of exclusions and limitations. For example, many state breach notification laws include exemptions from notification if an entity complies with obligations under sector-specific federal laws, such as HIPAA or the GLBA. In some cases, state privacy laws have carveouts for entities or individuals that are subject to sector-specific federal laws. For example, California's CCPA excludes, to various degrees, data that is governed by HIPAA, the GLBA, the FCRA, and other state and federal laws. Most other U.S. state privacy laws include similar carveouts.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

At the federal level, COPPA governs the collection, use and disclosure of personal information collected from children under the age of 13 by operators of websites and other online services. COPPA is primarily enforced by the FTC, which takes a broad view of COPPA's scope, applying it to many different types of online services (including video games, websites, connected toys and other internet-connected devices) and operators (including third-party contractors, advertisers and others who passively collect children's personal information). COPPA requires transparent and accessible privacy policies; heightened security practices to safeguard children's personal information; verifiable parental consent before collecting, using or disclosing personal information from a child, with narrow exceptions, including for internal operational purposes, one-time responses, and email verification; and rights for parents to access the information collected from children and to withdraw consent at any time.

In the educational context, FERPA protects the personal information from a student's educational record and applies to all educational institutions that accept federal educational funding, including kindergarten12 as well as institutions of higher education. FERPA sets forth how parents and students may access, correct, or delete student educational information and limits the disclosure of students' educational information without the consent of the student, or if the student is under 18, consent of the parent or legal guardian, or pursuant to another enumerated exception, such as disclosure to an online service provider acting as a "School Official" subject to the direction and control of the school. FERPA is supplemented by student data privacy laws passed in more than 40 states that govern schools' and thirdparty contractors' collection, use, disclosure and sale of student data collected or generated in connection with educational technology or services in a school setting.

A handful of state comprehensive privacy laws specifically address the collection and use of children's or minors' personal information. For example, under California's CCPA, businesses may not sell personal data of California residents under the age of 16 without the minor or, in the case of children under 13, their parents', opt-in consent. Other state privacy laws in Connecticut and, once in effect, similar laws in Delaware, Florida, Montana, New Jersey, and Oregon require consent from the parent (for minors under 13) or consent of the minor (for minors between 13 and 15, 16, 17, depending on the state) for certain types of processing activities, such as data sales, targeted advertising or profiling purposes. Once in effect, Florida's Digital Bill of Rights will require consent of the minor under age 18 for all processing activity. In addition, the state privacy laws in Colorado, Connecticut, Virginia and others not yet in effect treat the personal data of a child under 13 as "sensitive personal information," requiring a risk assessment or data protection impact assessment before processing takes place.

In addition, certain states have passed privacy laws specific to minors. California's Privacy Rights for California Minors in the Digital World law allows California residents under the age of 18 to delete publicly available personal information they have posted online. Connecticut's law concerning minors and online services, which is set to take effect October 1, 2024, applies to controllers who offer an online service, product or feature to consumers whom the controller has actual knowledge are under the age of 18. Connecticut's law requires consent from the minor (age 13-17) or the minor's parent (under age 13) before processing the minor's personal information for targeted advertising, data sales, or profiling activity, or the use of any system design feature that is designed to significantly increase, sustain or extend the minor's use of the service. The law also imposes restrictions on the collection of precise geolocation and direct messaging features, obligates the controller to use reasonable care to avoid heightened risk of harm to minors, and requires data protection impact assessments, among other requirements. Similarly, California's recently passed the California Age-Appropriate Design Code, modeled after the U.K. Age Appropriate Design Code framework, imposes a range of obligations on businesses that provide online products, services or features that are "likely to be accessed by children" under the age of 18, including requiring businesses to establish the age of a user with a reasonable level of certainty, conduct data protection impact assessments, implement default privacy settings to offer a high level of privacy, and provide an obvious signal to children when they are being monitored or tracked. The law was set to take effect on July 1, 2024, however, the law was challenged on constitutional grounds and preliminarily enjoined from taking effect, as of the date of this publication. Congress and numerous other states are considering children's online privacy and safety legislation this year.

12. Do the data protection laws in your jurisdiction address online safety? Are there any

additional legislative regimes that address online safety not captured above? If so, please describe.

Yes, in addition to the privacy laws set forth above, several states have also implemented laws addressing online safety. For example, Arkansas, California, Florida, Ohio, Utah, Connecticut, Louisiana, and Texas have all enacted legislation governing minor's use of social media, online games or other online services with social, interactive components, though California's Age-Appropriate Design Code and one of two Connecticut laws apply more broadly to any online services used by a minor. Most of these online safety laws were or are set to come into effect in 2024, though some are currently enjoined (Arkansas, California, Ohio) on First Amendment grounds. It remains to be seen whether and how courts will uphold the laws as drafted, and what effect these injunctions will have on dozens of similar legislative proposals pending on other states.

The State online safety laws' definition of what constitutes a "child" or "minor" range from up to age 16 (*e.g.*, Louisiana, Ohio) to up to age 18 (*e.g.*, Arkansas, California, Florida, Utah, Connecticut, and Texas). The laws generally regulate minors' use of social media or any online service or product that targets children or is reasonably anticipated to be accessed by children. Whether a business falls within the ambit of these online safety laws depends on the nature of the service or product being offered, its design elements, and whether the business knows or should reasonably know that the application or service is used by minor or has actual knowledge that a user is a minor. A few online safety laws contemplate or require some form of age verification or age assurance before a minor can create an account on a social media or online gaming service (*e.g.*, Arkansas, California, Florida, Louisiana, Texas, Utah, Ohio).

While the specific requirements of each state online safety law vary, they generally require controllers to implement or impose some or all of the following:

- A process to verify users' age prior to permitting use of the services or products;
- Verifiable parental consent mechanism for account creation or for certain features or processing activities;
- Data minimization, data retention limits and limitations on the collection of children's data to the purposes for which the data was collected;
- Limitations on direct messaging functionalities;
- Limitations on the use children's data for targeted advertising;
- Restrictions on the use or collection of geolocation data;
- Limitations on the use children's data for profiling, subject to certain exceptions;
- Measures to address risks to children's physical and mental health, including "addictive" or "excessive use" features; and
- Prohibitions on the use of dark patterns.

In addition, at least nine states have recently passed laws protecting minors from harmful online content, including Arkansas, Louisiana, Mississippi, Montana, North Carolina, Texas, Utah, Virginia, and Indiana. These laws typically apply to commercial websites or online services that contain a substantial portion (more than 33%) of material that is harmful to minors, such that the average person would find to appeal to the prurient interest, or material that exploits or principally consists of actual or simulated sexually explicit nudity, sexual content or other material that is patently offensive with respect to minors and lacks serious literary, artistic, political or scientific value to minors. These laws require in-scope online services to employ various age verification techniques to ensure minors under age 18 cannot access the harmful materials.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

At the federal level, the FTC is the primary regulator of online privacy laws, though certain sector-specific laws are enforced by other federal agencies (*e.g.*, the U.S. Department of Education oversees FERPA). Generally, the FTC has authority to bring enforcement actions related to companies' data processing practices under Section 5 of the FTC Act, which prohibits deceptive or unfair practices in or affecting commerce, or to enforce compliance with a regulation under the FTC's enforcement authority, such as the FTC's COPPA Rule. The FTC's enforcement powers include, among others, imposing injunctive relief on unauthorized activity, issuing cease-and-desist orders, and disgorgement or restitution remedies, and in some cases, civil penalties of $51,744 per violations of an FTC Rule. Any company that violates an order or an injunction that resulted from a related FTC action may be subject to civil penalties or sanction for contempt of court. States Attorneys General may also pursue investigations and

enforcement under COPPA, though typically under the State's own unfair and deceptive practices statute which provides for lower civil penalties.

At the state level, state attorneys general and in California, the California Privacy Protection Agency, are responsible for enforcing state privacy laws and state online safety laws and have the power to enjoin unauthorized activity or impose civil penalties, which vary by state. The magnitude of such penalties may depend on the nature of the violation and the age of the population subject to the alleged violation. For example, Florida's bill related to the protection of children in online spaces allows for civil penalties to be tripled in the event that a covered business has actual knowledge that its violation involves a Florida resident under the age of 18. State regulators may pursue an action independently or as part of a coordinated multi-state action investigation. State regulators may also partner with the FTC or other federal agencies to pursue enforcement action under various theories of liability, including for violations of state law that also constitute a violation of Section 5 of the FTC Act.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

The online safety landscape will continue to evolve through 2024 – 2025 as states continue to enact related legislation. In a January 2024 notice of proposed rulemaking, the FTC issued proposed revisions to the COPPA Rule, COPPA's implementing regulations that were last updated in 2013, subject to a public comment period that runs through March 11, 2024. Further, several states have online safety bills pending and federal legislators have surfaced several bipartisan drafts, including the *Kids Online Safety Act (KOSA)* and the *Children and Teens' Online Privacy Protection Act* (referred to as COPPA 2.0). We expect online safety to remain at the forefront of both the federal and state legislative agendas in the coming year.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

U.S. data protection law generally does not impose express data protection by design or by default requirements. However, each of the CPRA, VCDPA, CPA, CTDPA, UCPA, ICDPA, OCPA, TDPSA, MCDPA, DPDPA, TIPA, INCDPA, NJDPA, NHPA, and FDBR impose purpose or collection limitations on controllers, codifying aspects of the FIPPs and the European Union (EU) and UK General Data Protection Regulation (GDPR) data protection by design and by default principles. For example, the CPRA and the VCDPA include an explicit and overarching purpose limitation, requiring the collection and use of personal information to be bounded by principals of necessity, proportionality, and compatibility. The VCDPA also limits controllers' collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. The CPA imposes a similar limitation, as will the OCPA, TDPSA, MCDPA and FDBR when they come into effect.

However, the FTC has recommended that businesses consider both privacy and data security when designing and developing their products and services. In cases where a business is launching a novel product that raises unique privacy and data security issues, it is a best practice to take into consideration both privacy and data security impacts at the design stage.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Neither controllers nor processors of personal data are generally required to maintain any internal records of their data processing activities or to establish internal processes or written documentation under U.S. data protection law. However, several statutory frameworks, including the GLBA, HIPAA, and certain state information security and health laws, do set out specific record retention and written information security programs. These programs typically require internal processes reflecting and documentation of administrative, technical, and physical safeguards that are designed to protect the confidentiality and security of personal data processed by the business. For example, HIPAA requires covered entities to maintain related documentation for six years from the date of creation or from the date the policy was last in effect, whichever is later. Businesses typically use industry or third-party benchmarking data to determine how best to maintain records, including data processing documentation. Creating and maintaining data processing inventories can aid in compliance efforts when a business is required to disclose to consumers or

a regulator how it collects, uses, or discloses personal data, as well as the sources or recipients of the personal information, as is generally required under U.S. state privacy laws.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

Several sector-specific U.S. laws impose data retention and disposal obligations. For example, the NYDFS Cybersecurity Regulation requires companies to implement policies and processes to safely dispose of sensitive information. Under COPPA, an operator of an online service must retain children's personal information for only as long as is necessary to serve the original purpose for which it was collected and, thereafter, the operator must delete the information using reasonable measures to protect against its unauthorized access or use. Although HIPAA does not include any retention requirements for medical records, that the law requires covered entities to record any policy, procedure, action, or assessment carried out to comply with HIPAA for a minimum of six years from the date of their creation or, in the case of a policy, six years from when the policy was last in effect. BIPA also requires covered entities in possession of biometric identifiers or biometric information to establish a written data retention schedule and destruction guidelines pursuant to the law's requirements. Certain U.S. state privacy laws also require businesses to retain data for specific periods of time. For example, the CCPA requires controllers to maintain a record of all requests for at least 24 months, including all signed declarations used for the verification of consumers' identities.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

Consultations with regulators regarding privacy and data security matters are not generally required in the United States, and unlike in other countries, U.S. regulators are not data protection authorities of general application. Entities in certain regulated industries, such as health or financial services, may have routine or compulsory consultations with their federal or state regulators that include discussions concerning privacy or data security matters. Although not formally recommended in most cases, it may be advisable to consult with a regulator under certain circumstances.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

While periodic risk assessments are often advisable, data security risk assessments at the federal level are currently required for only business operating in certain industries and in a limited number of jurisdictions. For example, the NYDFS Cybersecurity Regulation requires regulated financial institutions and insurers to conduct risk assessments and implement an information security program based on assessment findings. Similarly, HIPAA requires covered entities and business associates to conduct periodic risk assessments and implement risk management plans based on such assessments. Similarly, the FTC amended the GLBA Safeguards Rule to require financial institutions to establish, as part of their security program, continuous monitoring or periodic penetration testing and vulnerability assessments. Tabletop exercises can assist a business handling personal data to train personnel and determine weak spots in data security policies and systems, notably in the context of a data security incident. Privacy impact assessments are not mandated by law in the United States as they are in other countries. However, the FTC and many state attorneys general have advised the adoption of privacy-by-design and use of privacy impact assessments as a best practice.

At the state level, with notable exception of the UCPA, the CCPA, VCDPA, CPA, and CTDPA and, once fully operative or effective, the OCPA, DPDPA, TIPA, TDPSA, INCDPA, MCDPA, NJDPA, and FDBR will require some form of a risk assessment. In particular, the VCDPA, CTDPA, CPA, OCPA, TDPSA, MCDPA, NHPA, and FDBR require controllers to conduct and document a data protection assessment for the processing of personal data for purposes of sensitive data, targeted advertising, and profiling that presents certain reasonably foreseeable risks to the consumer, the sale of personal data, and any activities involving personal data that present a heightened risk of harm to consumers. The CCPA calls for regulations (which are not yet finalized) setting out the contours of annual risk assessments and cybersecurity audits for businesses whose personal data processing presents a significant risk to consumer privacy or security. Any CCPA risk assessment will need to evaluate whether the business' processing involves sensitive

personal data and weigh the benefits of the processing (to the business, the consumer, other stakeholders, and the public) against the risks to the consumer. The CCPA's risk assessment requirement evokes the GDPR concept of the data protection impact assessment but goes further by requiring that such assessments be submitted to a regulatory body, the CPPA, on a regular basis. Certain other U.S. state privacy laws require that risk assessments be submitted upon the Attorney General's request, generally where relevant to an investigation.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

U.S. privacy laws do not require appointment of a data protection officer. However, it is a common practice for the FTC and state attorneys general to require as part of the settlement of an enforcement action that a business hire a chief privacy officer with C-suite level authority and a direct reporting line to the chief executive officer or the board of directors, and that it develop and maintain robust privacy and data protection policies and practices. HIPAA requires covered entities to designate a privacy officer and a security officer, and business associates to designate a security officer (though in practice, many business associates also designate a privacy officer to help implement their HIPAA compliance program). The privacy and security officers may also hold other titles and carry out unrelated duties. The privacy officer is responsible for overseeing the organization's development, implementation, and maintenance of HIPAA-compliant privacy policies and procedures for all health information that the business handles. The security officer implements policies and procedures to avoid, identify, contain, and resolve potential security risks to electronic health information. Both are responsible for ensuring that staff are properly trained on applicable HIPAA requirements.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

A number of U.S. federal and state data protection laws explicitly require employee training. For example, the HIPAA Privacy Rule requires covered entities to train all members of its workforce as necessary and appropriate to carry out their functions. HIPAA Security Rule requires covered entities to implement a security awareness and training program for all members of its workforce. The GLBA's Safeguards Rule also requires employee training, including a “qualified individual” responsible for implementing and enforcing the financial institution's information security program. FTC guidance on the Safeguards Rule encourages employee security awareness training and “regular refreshers.”

Similarly, PCI DSS requires that entities educate employees immediately after hire and at least annually on the business' obligations under PCI DSS. Entities subject to PCI DSS must also implement a formal security awareness program regarding the importance of cardholder data security. The security awareness program also requires training for staff with any security breach response responsibilities.

As an example at the U.S. state privacy law level, the CCPA requires businesses to ensure that all individuals responsible for handling consumer requests are “informed” of the statute's requirements and how to direct consumers to exercise their rights under the law.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

There is no omnibus federal law in the United States that requires entities to provide notice to individuals when collecting, processing, or disclosing personal data. However, the FTC, which serves as the closest thing the United States has to a lead data protection authority, takes the position that under Section 5 of the FTC Act, it is an unfair business practice not to disclose material data practices (most commonly in the form of a privacy notice), especially if the collection of personal data would be unexpected to the consumer. Further, any material omissions or inaccuracies in a privacy notice are deemed a deceptive practice.

Several federal sector-specific laws require privacy notices. For example, HIPAA requires covered entities to provide individuals a health information privacy notice titled a “Notice of Privacy Practices” and to obtain consent prior to certain types of disclosures of PHI. The GLBA requires financial institutions to provide annual privacy notices and to offer consumers certain privacy choices. Most states have their own versions of HIPAA and GLBA that may set higher standards. The Cable

Communications Policy Act requires cable communications providers to provide notice and obtain consent for to disclose subscriber information, except to the extent necessary to render core cable services. COPPA requires online service operators to post a privacy notice for parents and guardians and obtain consent prior to the collection of personal data from children. State insurance laws also regulate privacy notices and choices for insurers. Various state laws require privacy notices by internet service providers, and other states are considering similar legislation. Congress and various state legislatures are considering privacy and security requirements for Internet of Things (IoT) providers, some of which include privacy notice obligations.

Certain states data protection laws require privacy notices with broader applicability, including California, Nevada, Delaware, and Connecticut. For example, business-to-business (B2B) entities must post a privacy notice consistent with the Delaware Online Privacy and Protection Act ("DelOPPA"), while California and Nevada merely regulate consumer transactions and solicitations. Notably, California has a robust suite of privacy notice laws that require some form of privacy notice, including the California Online Privacy Protection Act of 2003 ("CalOPPA"), which requires online consumer services to post a privacy policy; Shine the Light law, which requires entities to post an online or offline privacy notice disclosing whether they share consumer personal data with third parties for the third parties' own direct marketing purposes; the Privacy Rights for California Minors in the Digital World law, which requires disclosures describing how a minor under age 18 can delete publicly available personal data that they have published online; and the CCPA, which requires specific disclosures, including information about consumers' rights with respect to their personal data. In fact, most U.S. state privacy laws require controllers to provide consumers with an accessible, clear, and meaningful privacy notice about its privacy practices and related consumer rights.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

Currently, U.S. data protection laws generally do not apply directly to processors; rather, most processor obligations are flow-down requirements imposed by controllers by contract. There are, however, several sector-specific federal laws (HIPAA, the GLBA, the FCRA, and COPPA) that require minimum standards for processors. In addition, federal procurement programs, such as the Defense Federal Acquisition Regulations Supplement ("DFARS"), may require entities servicing the federal government to maintain adequate security and apply protective measures to prevent the loss, misuse, or unauthorized access to or modification of information.

The CCPA regulates processors (termed "service providers") and sets out complex provisions regarding the disclosure of personal data to a vendor and whether such disclosure will be deemed a "sale" or "share," and when the service provider is entitled to a safe harbor as to a business' noncompliance with the law. Businesses should contract with service providers to establish the scope of permissible uses of personal data, as well as to develop a mechanism for flow-down obligations as it relates to consumer rights requests. The CPRA further expanded service provider contractual obligations and flow-down obligations, in particular by imposing specific contractual obligations on businesses that sell, share or otherwise disclose for a business purpose the personal data of a consumer to a third party, service provider or contractor. Although the CCPA already imposes contract obligations on businesses with respect to service providers and contractors, imposing contracting obligations vis-à-vis third parties significantly increased the scope and flow-down impact of the CPRA on business transactions. Further, the CPRA obligates not only businesses, but also, at least in some cases, service providers and contractors to pass consumer rights requests downstream to parties that have accessed the consumer's personal data.

Similar to the GDPR, other U.S. state privacy laws also make the controller and processor distinction and provide for affirmative obligations not only on controllers but also on processors. For example, under the VCDPA, processors are required to comply with a controller's instructions, to enter into the necessary data processing agreements with the controller, and to assist the controller in meeting its obligations under the law, including in relation to (i) consumer rights requests, (ii) protecting personal data; (iii) reporting any breach of personal data, and (iv) data protection assessments. Many other U.S. state privacy laws impose similar requirements on processors.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

Currently, most U.S. data protection laws do not require minimum contract terms with processors. However, there are several sector-specific federal laws (HIPAA, GLBA, FCRA, FERPA, COPPA) that may require processors' handling of personal data to be governed by written agreements that include specific provisions. Many U.S. state laws highly recommend that controllers contractually require processors to implement a written information security plan. California and Massachusetts require nonaffiliated service providers to contractually agree to take reasonable and appropriate measures to protect shared personal data, and Connecticut requires contractors working with the state to encrypt all sensitive personal data that is transmitted wirelessly or via public internet connection or that is visible on portable electronic devices. Some states also look to PCI DSS as the *de facto* benchmark for determining whether a service provider is sufficiently "secure" in the relevant context.

The CCPA, VCDPA, CPA, CTDPA, UCPA, ICDPA, OCPA, TDPSA, MCDPA, DPDPA, NJDPA, NHPA, and FDBR expand contracting obligations on controllers. For example, the CPRA created an overarching contracting requirement for businesses that sell, share, or otherwise disclose for a business purpose the personal data of a consumer to a third party, service provider, or contractor. The CPRA also created a new "contractor" designation and related contractor and service provider contracting obligations, significantly increasing the scope and flow-down impact on businesses' transactions. Similarly, the VCDPA, CPA, CTDPA, UCPA, ICDPA, OCPA, TDPSA, MCDPA, DPDPA, NJDPA, and FDBR require controllers to enter into a contract with all processors, which, among other things, must set forth instructions for processing personal data, the nature and purpose of processing, the type(s) of data subject to processing, the duration of processing and the rights and obligations of both parties. Processors also are obligated to enter into all required contracts with their respective controllers.

In the education law context, many state student privacy laws require specific contractual provisions between educational institutions and their service providers. For example, under California's state student privacy laws, a contract between a school and a third-party provider that fails to comply with the statutory contracting obligations will be rendered void and unenforceable.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

U.S. data protection laws generally do not have any direct diligence or assessment obligations relating to the appointment of processors. However, several sector-specific federal laws (HIPAA, the GLBA, COPPA) require controllers to obtain assurances that processors are capable of appropriately safeguarding covered data. Further, these laws require controllers to take reasonable steps to audit processors' maintenance of these standards. State privacy laws have varying requirements governing the contractual relationship between with processors to ensure compliance. For example, the CPA, CTDPA, DPDPA, INCDPA, MCDPA, OCPA, TIPA, TDPSA, VCDPA, NHPA, and NJDPA require processors to provide information reasonably necessary for the controller to conduct and document data protection assessments. Further, some of these states allow for annual inspections or audits of the processor's policies and technical and organizational measures. The CCPA permits controllers to monitor the counterparty's contractual compliance through ongoing manual reviews, automated scans, regular assessments, audits, or other technical and operational testing.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

Laws in the United States that apply to monitoring, automated decision-making, or profiling generally do not prohibit these activities, but rather regulate or require disclosures regarding the use of cookies and other tracking technologies. "Profiling" is typically defined as "automated processing" of personal data "to evaluate, analyze or predict" characteristics of a person's "economic situation, health, personal preferences, interests, reliability, behavior, location or movements." While the CCPA and ICDPA are silent about profiling and automated decision-making, the CPRA, VCDPA, CPA, CTDPA, DPDPA, FDBR, INCDPA, MCDPA, NHPA, NJDPA, OCPA, TIPA and TDPSA grant consumers certain rights to opt-out of the processing of their personal data for purposes of profiling and create requirements that regulate use of automated decision-making, including profiling.

In contrast, U.S. state consumer health privacy laws categorically prohibit certain kinds of profiling. The MHMD Act, Nevada's similar law, and the CTDPA prohibit the use of geofences—such as digital locationbased trackers that show ads according to a person's proximity to a designated location—when used to identify or track consumers seeking a broad array of "health care

services"; collect consumer health data; or send notifications or ads to a consumer related to their consumer health data or access of health care services.

Two federal statutes have been used to regulate the use of cookies for tracking and behavioral advertising, though they do not relate directly to cookies: specifically, the FTC Act has been used as a basis for regulatory enforcement against entities misrepresenting or failing to disclose use of cookies for tracking purposes; the Federal Computer Fraud and Abuse Act ("CFAA") and its state equivalents have also been used as the basis of enforcement action against entities using cookies for behavioral advertising, where the cookie allowed for deep packet inspection. Some states have also enacted deceptive practices laws that have been used as a basis for similar enforcement: for example, the city attorney for Los Angeles brought a claim under California's consumer protection laws against the Weather Channel for disclosing users' geolocation data to advertisers and others without clear and conspicuous notice or express consent. Moreover, certain state laws impose disclosure obligations as to the use of or disablement of tracking technologies: for example, under CalOPPA, entities are obligated to disclose in their online privacy policy whether the website responds to "Do Not Track" signals and whether third parties may collect personal data across time and services using tracking technologies on the site. Similarly, the CCPA requires businesses in their online privacy policy to disclose with whom they sell personal data, including data gathered from first- or third-party cookies and other tracking technologies. The CPRA expanded consumers' right to opt-out of a business's "sharing" of personal data with a third party for purposes of cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

In addition, the ECPA, SCA, CFAA, and their state law equivalents, as well as tort laws, have been used as a basis for lawsuits against companies utilizing keystroke and other tracking features on websites and mobile apps, such as session replay technology. There has been a recent wave of class action litigation brought under California's Invasion of Privacy Act ("CIPA") and Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA") against companies for their use of such technologies. In these cases, the plaintiffs generally assert that (i) vendor tracking technologies on a business' website constitutes unlawful recording of the plaintiff's interaction with the business, and (ii) the business is aiding, agreeing with, employing or conspiring with the vendor to undertake such unlawful recording activity.

Finally, the Digital Advertising Alliance and the Network Advertising Initiative's self-regulatory programs for the U.S. digital advertising industry require notice, enhanced notice for intrusive or sensitive tracking, and an opportunity to opt-out.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

Virtually all U.S. state privacy laws provide consumers the right to opt-out of the processing of personal data for purposes of cross-contextual behavioral advertising, also referred to as targeted advertising, subject to certain exceptions.

The CCPA defines cross-contextual behavioral advertising as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts." The CCPA also provides consumers a related right to opt-out of a business' "sharing" of their personal data to a third party for cross-contextual behavioral advertising, whether or not for monetary or other valuable consideration.

U.S. comprehensive state privacy laws have nearly identical definitions of the equivalent "targeted advertising," which means displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained over time from the consumer's activities across nonaffiliated websites, applications or online services to predict the consumer's preferences or interests. The CPA, DPDPA, MCDPA, NHPA, and NJDPA expand the definition to include personal data "obtained *or inferred*" over time. Notably, the CPA, CTDPA, DPDPA, FDBR, INCDPA, MCDPA, NHPA, NJDPA, OCPA, TIPA, TDPSA, and VCDPA require controllers who process personal data for purposes of targeted advertising to conduct and document data protection assessments in certain circumstances.

U.S. state consumer health privacy laws categorically prohibit geofencing certain persons or entities that provide in-person health care services for purposes of advertising to consumers based on their consumer health data or access of health care services or products. The MHMD Act prohibits such geofencing within 2,000 feet of any person or entity that provides in-person health care services. Nevada's similar consumer health data law expands the prohibition to include persons or entities

providing health care products, at a geofence of 1,750 feet. The CTDPA similarly prohibits geofences within 1,750 feet, though limits the restriction to only mental, reproductive or sexual health facilities.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

Virtually all U.S. state privacy laws address the sale of personal data. For example, the CCPA broadly defines "sale" to mean the selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal data by the business to another business or third party for monetary or other valuable consideration. While this definition may be broad, the CCPA outlines a number of exceptions, including where the business shares the data with a service provider as necessary to perform a "business purpose." If the business sells a consumer's personal data, the consumer has the right to opt-out of this sale and the business is obligated to provide information about this right to consumers in the business's privacy notice, and a link titled, "Do Not Sell or Share My Personal Information" or "Your Privacy Choices" must be included on the business's internet homepage, if applicable. The CPRA expands on the CCPA's existing opt-out rights to include the right to opt-out of the "sharing" of personal data. "Sharing" is defined by the CPRA to mean the transfer or making available of a "consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration." Under the CPRA, businesses are prohibited from selling or sharing personal data of a consumer under the age of 16 unless the consumer (for consumers at least 13 years old) or the consumer's parent (for consumers under 13) have affirmatively authorized such sale or sharing.

The CPA, CTDPA, NPL, UCPA, VCDPA and, once effective, the DPDPA, FDBR, ICDPA, INCDPA, MCDPA, NHPA, NJDPA, OCPA, TIPA and TDPSA will similarly require businesses to offer consumers the right to optout of the sale of their personal data, though each defines "sale" slightly differently. The CPA, CTDPA, DPDPA, FDBR, MCDPA, NHPA, NJDPA, OCPA and TDPSA define "sale" to mean the exchange of personal data for monetary or other valuable consideration by a controller to a third party, whereas the VCDPA, UCPA, ICDPA, INCDPA, NPL and TIPA, define "sale" to mean the exchange of personal data for monetary consideration by a controller to a third party.

U.S. state consumer health privacy laws impose similar "sale" restrictions, commonly defined as the exchange of consumer health data for monetary or other valuable consideration. The MHMD Act and Nevada's similar law require covered entities to obtain detailed written authorization from a consumer prior to selling or offering to sell consumer health data. This authorization must be separate and distinct from the consent obtained to collect consumer health data, meet an enumerated list of specific content requirements, and would only be valid for one year. In contrast, the CTDPA prohibits the sale or offering of a sale without first obtaining affirmative consumer consent, a much less stringent standard.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

In the United States, federal and state laws regulate the way in which companies communicate with individuals and other businesses for marketing purposes. In particular, these laws regulate the ways in which companies can call, text or fax consumers.

Telephone communication (including telemarketing calls, autodialed calls, and prerecorded calls), text messages, and fax communications are regulated by the TCPA, the Telemarketing Sales Rule, and equivalent state laws. The rules pertaining to such communications differ according to the type of communication at issue, such as marketing versus non-marketing communications. On December 13, 2023, the Federal Communications Commission ("FCC") adopted new rules under the TCPA that require comparison shopping websites, lead generators, and other companies obtaining consent on behalf of third parties to obtain a consumer's prior express written consent to receive robocalls and robotexts one marketing partner at a time. On February 8, 2024, the FCC also announced that calls that use AI-generated voices are subject to a number of obligations and restrictions under the TCPA: these include securing prior express written consent before using an "artificial or prerecorded voice" in marketing calls to residential or cellular lines; issuing related disclosures; and providing an automated, interactive mechanism to optout of such calls.

Email communications are regulated by the federal CAN-SPAM Act, which establishes requirements for sending

unsolicited commercial email and giving consumers the right to opt-out of commercial email through prompt compliance with any unsubscribe request. The CAN-SPAM Act preempts state law, except to the extent they prohibit fraud or deception. Generally, the TCPA is mostly an opt-in scheme, while the CAN-SPAM Act takes an opt-out approach. Both require certain notices and disclosures and have various other requirements. Email communications may also be protected by ECPA and SCA, which together address interception and compelled disclosure of various electronic communications.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

In the United States, state laws regulate the way in which companies may process "biometric information." Illinois, Texas, and Washington currently have biometric-specific privacy laws. Similar laws have recently been proposed in Colorado, Hawaii, Kentucky, Maine, Massachusetts, Minnesota, Missouri, Nebraska, New Jersey, New York, Oklahoma, Pennsylvania, Tennessee, and Vermont. Additionally, a number of U.S. cities that have enacted their own facial recognition laws, such as New York City, Boston (Massachusetts), Seattle (Washington), Portland (Oregon), and Baltimore (Maryland). Washington and Nevada's consumer health privacy laws include biometric data within their respective definitions of "consumer health data."

Illinois' BIPA is uniquely strict. While the Washington and Texas laws apply to biometric information that is collected or used for commercial purposes, BIPA captures any collection or use by a private entity. Additionally, while civil penalties may be imposed for violations under all three states' biometric privacy laws, only BIPA provides for a private right of action by an affected individual (*e.g.*, an employee or customer). This has made Illinois a hotbed for class action litigation directed at businesses based on the collection and use of biometric information without consent, including in the employment context.

BIPA defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." Several categories of information are expressly excluded from this definition, such as photographs, human biological samples used for scientific testing or screening, demographic data, physical descriptions of people or any data captured in a health care setting or subject to HIPAA. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify an individual." Biometric information excludes information derived from items that are excluded from the definition of a biometric identifier.

There are five main obligations under BIPA: an entity (i) must create and adhere to a public, written policy on retention and destruction of biometric information and biometric identifiers (collectively, "biometric data"); (ii) prior to the collection of biometric data, must provide notice and obtain a "written release," defined as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment"; (iii) must either obtain consent from or be authorized by an individual to disclose biometric data; (iv) cannot sell, lease, trade or otherwise profit from a person's or a customer's biometric data; and (v) must implement reasonable security measures for the storage or transmission of biometric data.

As mentioned above, a violation of BIPA can result in significant litigation costs, as BIPA allows for a private right of action. Any person aggrieved by a violation may recover:

- Liquidated damages of $1,000 (or actual damages if greater) per negligent violation;
- Liquidated damages of $5,000 (or actual damages if greater) per intentional violation; and/or
- Reasonable attorneys' fees and costs.

All state comprehensive data privacy laws enacted to date address the processing of biometric data. Most of these laws define biometric data as "data generated by automatic measurements of an individual's biological characteristics," such as fingerprints, voiceprints, eye retinas, and irises. The CCPA defines "biometric information" more broadly, as "an individual's physiological, biological, or behavioral characteristics."

Each state data privacy law regulates the processing of biometric data by including it in the statutory definitions of "sensitive data" or "sensitive personal information." That said, the CPRA, CTDPA, DPDPA, FDBR, ICDPA, INCDPA, MCDPA, NHPA, TIPA, TDPSA, UCPA, and VCDPA consider biometric data to be sensitive data only when it is processed for the purpose of uniquely identifying an individual. In contrast, sensitive data under the CPA, NJDPA, and OCPA is defined to include biometric data to the extent that such data *may* be processed for the purpose of uniquely identifying an individual.

Of note, at the federal level, the FTC has increased its focus on unfair and deceptive trade practices in relation to facial recognition technology, previously going as far as declaring it "discriminatory and dangerous." The FTC continues to investigate facial recognition-related activities.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

In the United States, most comprehensive state privacy laws provide consumers with the right to direct controllers not to use automated decision-making or profiling for certain purposes. "Profiling" is typically defined as "automated processing" of personal data "to evaluate, analyze or predict" characteristics of a person's "economic situation, health, personal preferences, interests, reliability, behavior, location or movements." The CPA, CTDPA, DPDPA, FDBR, INCDPA, MCDPA, NHPA, NJDPA, OCPA, TIPA, TDPSA, and VCDPA allow consumers to opt-out of the automated processing of personal data for purposes of profiling in furtherance of decisions producing legal or similarly significant effects. Such effects typically include decisions that result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

The CPRA defines profiling as any automated processing of personal Information "to analyze or predict" individual characteristics, including but not limited to a person's "performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." The CPRA directs the adoption of regulations governing access and opt-out rights regarding the use of automated decision-making technology, including profiling. Additionally, the regulations will address responses to access requests, including providing meaningful information about the logic involved in the decisionmaking process, as well as a description of the likely outcome of the process with respect to the California resident. The CPPA Board intends to advance its proposed automated decision-making technology regulations to formal rulemaking in July 2024.

States have also enacted laws to further regulate AI technologies in specific contexts: California prohibits deceiving a chatbot user regarding the artificial identity of the chatbot in order to incentivize a purchase or influence a vote. Utah subjects the use of generative AI in certain professional contexts to the oversight of the state's Division of Consumer Protection and imposes disclosure requirements on use of the technology to communicate with consumers or to create political advertisements. Illinois, Maryland, and New York each regulate certain uses of AI in employment decision-making contexts. Colorado regulates the use of algorithms and predictive models in insurance practices that unfairly discriminate based on certain protected characteristics. As of publication, several other state legislatures are considering laws that would govern use of AI and machine learning.

At the federal level, the Biden Administration in October 2023 announced Executive Order 14110, establishing standards for AI safety. The order included a mandate to the Department of Commerce to develop guidance for content authentication and watermarking to clearly label AI-generated content. Accordingly, federal agencies have taken an increased interest in AI. On February 8, 2024, the FCC announced that calls that use AI-generated voices are subject to a number of TCPA obligations and restrictions: these include securing prior express written consent before using an "artificial or prerecorded voice" in marketing calls to residential or cellular lines, as well as providing various disclosures and an automated, interactive mechanism to opt-out of such calls. In addition, the FTC has sought to address issues raised by business' retroactive use of consumer data for purposes of training third party or in-house AI tools by issuing a statement informing consumers of their more permissive data practices through surreptitious, retroactive amendments to terms of service or privacy policies. The FTC has issued a statement characterizing such actions as potentially constituting an unfair or deceptive trade practice.

32. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

The United States does not currently have any data transfer or data localization requirements. If data is processed outside the United States, however, that fact should be disclosed in the business's privacy policy.

Notwithstanding, on February 28, 2024, President Biden issued Executive Order 14117, which delegates new authorities to the U.S. Department of Justice ("DOJ") and other agencies to regulate the transfer of certain

categories of sensitive personal data and U.S. government-related data to "countries of concern," as defined in the order. The DOJ has issued a corresponding Advance Notice of Proposed Rulemaking outlining the contemplated regulatory regime that will prohibit or restrict certain transactions by U.S. persons and companies that involve such categories data. The order requires the DOJ to publish a proposed rule by August 26, 2024.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

While the nature and scope of security obligations in the United States are still developing, many U.S. data protection laws mandate at least "reasonable and appropriate security measures." At the federal level, this requirement is found in certain sector-specific statutes and regulations. FTC guidance also advises entities to implement a "comprehensive security program that is reasonably designed to address security risks" and "protect the privacy, security, confidentiality, and integrity" of consumers' information. The FTC has taken the position that this security requirement applies broadly to all companies under its jurisdiction by way of the FTC Act, although this is disputed. In a series of FTC enforcement actions, the FTC has asserted that its security programs standard has been required to address a wide range of potential risks, including:

- employee training and management;
- product design, development and research;
- secure software design, development, and testing, including for default settings, accessing key and secret key management, and securing cloud storage;
- application software design;
- information systems, such as network and software design, information processing, storage, transmission and disposal;
- replacement of inadequate authentication measures, minimization of data retention and application of readily available protections against well-known threats;
- providing consumers access to data collected about them and allowing them to request the deletion of their data;
- reviewing, assessing and responding to third-party security vulnerability reports; and
- preventing and detecting and responding to attacks, intrusions or other systems failures and vulnerabilities.

Following the identification of security risks, FTC guidance would require entities to:

- design and implement "reasonable safeguards" to control for the identified risks;
- conduct regular testing of the effectiveness of key controls, systems and procedures, and evaluate and adjust information security programs based on the results of the testing;
- implement a written information security policy;
- adequately train personnel to perform data security-related tasks and responsibilities;
- ensure that third-party service providers implement reasonable security measures to protect personal information, such as through the use of contractual obligations;
- regularly monitor systems and assets to identify data security events and verify the effectiveness of protective measures;
- track unsuccessful login attempts;
- secure remote access;
- encrypt certain personal data;
- replace inadequate authentication methods with multifactor authentication methods;
- restrict access to data systems based on employee job functions;
- develop comprehensive password policies, addressing password complexity, prohibiting reuse of passwords to access different servers and services, and deploying reasonable controls to prevent the retention of passwords and encryption keys in clear text files on the company's network; and
- conduct vulnerability and penetration testing, security architecture reviews, code reviews and other reasonable and appropriate assessments, audits, reviews or other tests to identify potential security failures and verify that access to devices and information is restricted consistent with user security settings.

In addition, at least 25 states have laws that address data security practices of private sector entities, including many of the comprehensive state privacy laws (*e.g.*, Virginia, Colorado, Connecticut, Utah, and Iowa). Most of these state laws relate to entities that maintain personal data about residents of that state and require the entity to maintain "reasonable security procedures and practices" appropriate to the type of information and the associated risk. In California, the Customer Records Act requires certain companies to maintain reasonable security procedures and practices, and the CCPA provides for a

private right of action, which in certain circumstances may be brought as a class action for statutory damages, in connection with certain data security breaches that result from a violation of the duty to maintain reasonable security measures. In addition, the CCPA imposes on businesses an obligation to contractually obligate third parties with whom the business sells, shares or discloses personal data to provide the same level of privacy protection as required by the CCPA.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

All states in the United States, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted laws requiring notification in the event of a "security breach," "breach of security," or "breach of security of the system" (collectively referred to here as a "security breach"). These jurisdictions define security breach differently, but generally the definition is dependent on three elements: (1) the types of personal information protected by the relevant statute, (2) how an unauthorized person interacted with the protected personal information and (3) the potential that the incident could result in harm to the individuals whose protected personal information was involved.

The vast majority of the jurisdictions with breach notification laws define security breach to require unauthorized acquisition of personal data. A small number of jurisdictions, including Connecticut, Florida, New Jersey, New York, Puerto Rico, and Rhode Island, define a security breach as the unauthorized access to personal data. The remaining jurisdictions define a security breach as both unauthorized access to and acquisition of personal data. No state requires notification to individuals or regulators if an incident has not resulted in unauthorized acquisition of or access to personal data.

For a small number of states, the definition of security breach includes both computerized/electronic data and paper/hard copy records. For example, Indiana's definition of "breach of the security of data" includes "the unauthorized acquisition of computerized data that has been transferred to another medium, including paper, microfilm, or a similar medium […]"

Additionally, a majority of the jurisdictions maintain a risk-of-harm analysis, which, for some, is provided for in the definition of security breach. North Carolina's law, as a representative example, defines security breach as "an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer." Most jurisdictions also maintain an exception in the definition of security breach, which generally states that a good faith but unauthorized acquisition of personal data for a lawful purpose is not a security breach unless the personal data is used in an unauthorized manner or subject to further unauthorized disclosure.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

In the United States, "reasonable" security measures are required by many state and federal laws that are specific to particular sectors or types of personal data. Included below is a non-exhaustive list of industry specific security requirements at the federal level:

- HIPAA imposes privacy and security obligations on entities that handle PHI.
- GLBA imposes security standards designed to protect NPI maintained by financial institutions about their customers.
- The Cable Act, absent an exception, prohibits cable operators from disclosing personal information to third parties without the subscriber's consent and imposes a general data security obligation on covered entities to prevent unauthorized access to personal information.
- The Telecommunications Act of 1996 imposes privacy and security obligations on entities acting as common carriers, such as telephone services.
- COPPA requires covered entities to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."
- The Energy Policy Act of 2005 gave the Federal Energy Regulatory Commission (FERC) authority to oversee the reliability of the bulk power system, commonly referred to as the bulk electric system or the power grid. This includes authority to approve mandatory cybersecurity reliability standards.
- The North American Electric Reliability Corporation (NERC), which FERC has certified as the nation's Electric Reliability Organization, developed Critical Infrastructure Protection

(CIP) cybersecurity reliability standards. On January 18, 2008, FERC issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns.

- The Securities and Exchange Commission (SEC) has published various rules, and proposed rules, imposing specific security requirements for the securities industry. In March 2023, the SEC published a set of proposed new rules for Market Entities, which include broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers and transfer agents. The proposed rules seek to address cybersecurity risks through (i) policies and procedures, (ii) immediate notification to the Commission of the occurrence of a significant cybersecurity incident, (iii) reporting detailed information to the Commission about a significant cybersecurity incident and (iv) public disclosures that would improve transparency with respect to cybersecurity risks and significant cybersecurity incidents.

For federal government corporate and critical infrastructure networks and databases, former President Obama issued an Executive Order in February 2013, *Improving Critical Infrastructure Cybersecurity*, directing the National Institute of Standards and Technology ("NIST") in the U.S. Department of Commerce to develop the Cybersecurity Framework. The NIST Cybersecurity Framework provides voluntary guidance to assist organizations in identifying and managing critical infrastructure cybersecurity risks.

At the state level, for example, Illinois' BIPA requires reasonable security measures for businesses handling biometric data and the NYDFS Cybersecurity Regulation requires heightened data security safeguards for regulated financial institutions and insurers. The NYDFS Cybersecurity Regulation requires a covered entity and its third-party service providers to perform a risk assessment and subsequently create and maintain a cybersecurity program that address the findings of the risk assessment. The cybersecurity program must be designed to perform a set of core cybersecurity functions, such as developing and using a defensive infrastructure to protect against cyberattacks, as well as detecting and reporting cybersecurity events. Many states also have specific security requirements for state-licensed insurance businesses which are often modeled after the FTC's Safeguards Rule. Several states (such as California, Delaware, New York, Washington, and West Virginia) require by statute that state government agencies have security measures in place to protect state databases and secure critical infrastructure controls and information.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

In the United States, data breach notification requirements can be complex due to the variety of potentially applicable federal and state laws. All states in the United States, as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, have enacted laws requiring notification in the event of a security breach involving affected residents of that jurisdiction. The scope of what data is covered as well as the notice, timing and reporting obligations vary from state to state. Some of these laws contain substantially different definitions for what is considered a "security breach" and what is considered "personal data." To determine which state's law applies, a company must first determine the state of residence of the consumers whose information was affected and look to that state's law to evaluate the reporting requirements. Many state breach notification laws include exemptions from notification if an entity complies with obligations under sector-specific federal laws such as HIPAA and GLBA.

When a business becomes aware of an actual security breach, as that term is defined under the applicable law, it typically has a set amount of time (depending on the applicable state or federal law) to report it to the relevant consumer. In some states, there is also a requirement to report a breach to third parties (*e.g.*, state regulatory authority, state police and/or consumer reporting agency). Failure to notify and to report within the applicable time frame can result in fines and penalties under applicable law, and can give rise to reputational and other risks, such as litigation.

While there is presently no federal breach notification law applicable to the entire United States that requires businesses to report security breaches, there are

industry-specific requirements with which businesses must comply. For example, HIPAA-covered entities have up to 60 days to notify the appropriate federal authorities and affected individuals when 500 or more individuals have been affected. The GLBA requires businesses to notify affected individuals of a security breach "as soon as possible." In 2023, the SEC finalized rules requiring publicly traded companies to disclose a cybersecurity incident on a Form 8-K within four business days of determining such incident as "material," where such materiality determinations must be made "without unreasonable delay" after discovering an incident. Additionally, the NYDFS Cybersecurity Regulation requires registered financial institutions to report a security breach within 72 hours of becoming aware of the breach.

Notably, in March 2022, the Cybersecurity and Infrastructure Security Agency ("CISA") passed the Cyber Incident Reporting for Critical Infrastructure, which will require critical infrastructure companies to report any ransom payments or substantial cybersecurity incidents to the federal government within 24 and 72 hours, respectively. Many key details of the reporting requirements are subject to future rulemaking by CISA, including the critical infrastructure organizations to which the reporting requirements will apply; what cyber incidents must be reported (i.e., "substantial" cybersecurity incidents); what information critical infrastructure organizations will have to report; and the mechanics of submitting the reports. The proposed rules are required to be issued in the rulemaking process by March 2024, with the final rule due 18 months thereafter.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

While there is not a specific and directly applicable law that addresses cybercrime attacks in the United States, there are a number of other laws that may provide some guidance regarding ransomware attacks and the like.

At the federal level, if ransomware is used to intercept the transmission of personal information or access personal information stored in electronic communications, such as emails, it may result in an ECPA violation. Additionally, cybercrime attacks may be prosecuted under the CFAA, as long as there is evidence that there was an intent to cause harm or damages (i.e., the violator knowingly and intentionally spread the ransomware). Once effective, CISA's Cyber Incident Reporting for Critical Infrastructure will require critical infrastructure companies to report any ransom payments to the federal government within 24 hours. CISA has also issued the "SHIELDS UP" guidance to all organizations that provide steps on detecting, responding and reducing the likelihood of a damaging cyber intrusion, and maximizing the organization's resilience.

In September 2021, the U.S. Department of Treasury's Office of Foreign Asset Control ("OFAC") published its Updated Advisory on Potential Sanction Risks for Facilitating Ransomware Payments. The guidance emphasized that OFAC strongly discourages payment of ransom in connection with cyberattacks and that it will continue to impose sanctions on persons who materially assist, sponsor or provide financial, material or technical support for ransomware activities. In this Advisory, OFAC provided actions companies should take to mitigate the risk of an OFAC enforcement action, including: (1) adopting or improving cybersecurity practices to reduce the risk of cyber extortion; (2) self-initiated, timely and complete reporting of ransomware attacks to the U.S. government (which OFAC will also consider a voluntary self-disclosure); and (3) cooperating with OFAC, law enforcement and other relevant agencies. Finally, the Advisory underscored the importance of implementing a risk-based sanctions compliance program. In particular, companies that engage with victims of ransomware—including those that provide cyber insurance, digital forensics and incident responses, and financial services that may involve processing ransom payments—should account in their policies for the risk that a ransomware payment may involve a sanctions target.

At the state level, all 50 states have computer crime laws, and most of them are in relation to unauthorized access, spyware, phishing and ransomware. Notably, NYDFS recently amended its Cybersecurity Regulations to require covered entities to notify NYDFS within 24 hours of making an extortion payment in connection with a cybersecurity event. Further, within 30 days of making such a payment, the entity must also provide a written description of the reasons payment was necessary, a description of alternatives to payment considered, diligence performed to find payment alternatives, and diligence performed to ensure compliance with applicable regulations, including OFAC's advisories.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

No, the United States does not have a separate

cybersecurity regulator. Federal and state privacy laws are enforced by relevant federal and state regulators depending on the underlying statute.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, any exceptions and any other relevant details.

There is no single federal law in the United States that sets out an all-encompassing overview of available individual privacy rights. Rather, each of the various state privacy laws sets out the individual privacy rights available to the residents of those states. These consumer rights are not absolute and are limited by various exceptions. Note that not all of the laws discussed below are in effect as of the time of publication.

Right to Know

Generally, the right to know affords consumers the right to obtain certain details about the personal data that controllers collect about them. Upon receipt of a verifiable request to exercise the right to know, businesses may be required to confirm whether the controller is processing the consumer's personal data. The following state privacy laws afford the right to know to their respective state residents: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Iowa (ICDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), Utah (UCPA), and Virginia (VCDPA). In California, business may also be required to disclose to the consumer which specific pieces or categories of personal data is collected from the consumer, the sources of such information, the business or commercial purposes for collecting or further disclosing the data, and the categories of third parties to whom the business has disclosed their personal data. Moreover, in Oregon, consumers can request a list of the specific third parties to whom personal data is disclosed.

Right to Access

Generally, the right to access allows for a consumer to access the personal data collected about them. The following state privacy laws grant the right to access to their respective residents: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Iowa (ICDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), Utah (UCPA), and Virginia (VCDPA).

Right to Portability

Generally, consumers have the right to obtain a copy of their personal data in a portable, and to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means. The following state privacy laws grant the right to portability to their respective residents: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Iowa (ICDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), Utah (UCPA), and Virginia (VCDPA).

Right to Deletion

Generally, the right to deletion requires a controller to delete a consumer's personal data (including both data provided by or obtained about the consumer). The following state privacy laws grant their respective residents the right of deletion: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Iowa (ICDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), Utah (UCPA), and Virginia (VCDPA).

Right to Correction

Similar to the GDPR right of rectification, the right to correction requires a business to correct inaccurate personal data maintained about a consumer. Once a business receives a verified request to correct inaccurate personal data, the business must use “commercially reasonable efforts” to correct the data as directed by the consumer and the adopted regulations. The following state privacy laws grant their respective residents the right of correction: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), and Virginia (VCDPA).

Right to Limit or Control Over Sensitive Personal Data

Consumers have the right to exercise control over a controller's collection and processing of their sensitive personal data. This generally includes a requirement that consumers expressly consent (or in the case of a child,

their guardian expressly consent) to the processing of their sensitive personal data. The following state privacy laws grant their respective residents the right to limit or control the processing of sensitive data: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Iowa (ICDPA), Montana (MCDPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), Utah (UCPA), and Virginia (VCDPA).

Right to Control Over Automated Decision-Making or Profiling

Generally, state privacy laws afford consumers the right to direct controllers not to use automated decision-making or profiling for certain purposes. Generally, consumers have the right to opt-out of such processing of data that produce a legal or similarly significant effect—that is, a decision that results in the provision or denial by the controller of, for example, financial and lending services, housing, insurance or health care services, education enrollment, employment opportunities, criminal justice, or access to basic necessities. Automated decision-making involving sensitive data requires consumers to opt in prior to such processing of data. The following state privacy laws afford their respective residents the right of control over automated decision-making or profiling: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), and Virginia (VCDPA).

Right to Opt-Out of Voice and Facial Recognition Features

Florida residents under the FDBR are afforded the right to opt-out of the collection of their personal data through the operation of a voice recognition or facial recognition feature.

Right to Opt-Out of Targeted Advertising

Consumers generally have the right to opt-out of the processing of personal data for purposes of targeted advertising (or, similarly, the sharing of personal data with a third party for purposes of crosscontext behavioral advertising). The following state privacy laws grant their residents the right to optout of targeted advertising: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Iowa (ICDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), Utah (UCPA), and Virginia (VCDPA).

Right to Opt-Out of Sales

State privacy laws generally afford consumers the right to opt-out of the sale of their personal data to third parties for monetary or other valuable consideration, as described above. The following state privacy laws grant to their respective residents the right to opt-out of sales: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Iowa (ICDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), Utah (UCPA), and Virginia (VCDPA).

Right to Non-Retaliation

Consumers have the right to not receive retaliatory or discriminatory treatment for exercising their individual privacy rights. Consumers need not specifically request to exercise this right. The following state privacy laws grant their respective residents the right to non-retaliation: California (CCPA), Colorado (CPA), Connecticut (CTDPA), Delaware (DPDPA), Florida (FDBR), Indiana (INCDPA), Iowa (ICDPA), Montana (MCDPA), New Hampshire (NHPA), New Jersey (NJDPA), Nevada (NPL), Oregon (OCPA), Tennessee (TIPA), Texas (TDPSA), Utah (UCPA), and Virginia (VCDPA).

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

The individual data privacy rights afforded under U.S. state privacy laws are generally enforced by U.S. state attorneys general. Notably, individual rights under the CCPA may be enforced by the California Attorney General's Office or, in certain cases described above, through a private right of action. Further, the CPRA has newly designated the CPPA as the CCPA's lead enforcement agency—notably, however, the CPRA does not strip the California Attorney General of all enforcement authority. Thus, a business violating the CCPA as amended may alternatively be subject to an injunction and civil penalty in an action initiated by the California Attorney General.

Otherwise, most state privacy laws delegate enforcement responsibility to the state attorney general, including Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Hampshire, New Jersey, Nevada, Oregon, Tennessee, Texas, Utah, and Virginia. Of exception, in Utah, the Division of Consumer Protection may consult with the Utah Attorney General and assist with enforcement of the UCPA; in Colorado, the Colorado Attorney General has

concurrent authority to enforce the CPA with district attorneys.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Currently, there is no comprehensive federal U.S. data protection law that provides for a private right of action for privacy violations; that said, several federal and state data protection laws do afford for private rights of action in limited circumstances: for example, Illinois' BIPA affords individuals whose biometric data is collected or handled without authorization to bring a private right of action against the responsible business. Certain state personal data breach notification laws requiring "reasonable" security also have a private right of action for violations of the same: for example, the CCPA allows consumers to institute a civil action where certain of the consumer's non-encrypted and non-redacted personal data is subject to "unauthorized access and exfiltration, theft or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information […]." Notably, the CPRA added an email address in combination with a password or security question plus answer to the list of data elements that, if breached, could give rise to a private right of action, and clarifies that maintaining reasonable security procedures does not amount to a "cure" under the law (thus narrowing the pre-action notice-and-cure requirement). Also at the state level, the MHMD Act enables plaintiffs to bring an action against businesses under Washington's Consumer Protection Act.

At the federal level, a private right of action is afforded to certain recipients of telephone calls, text messages or other applicable communications that violate the TCPA. The FCRA provides a private right of action for the mishandling of consumer background checks or the printing of excessive payment card information on receipts. The VPPA provides a private right of action for certain disclosures of video rental information.

In addition, private plaintiffs have had mixed results in asserting general theories of liability in connection with privacy and cybersecurity practices, including negligence, breach of contract, common-law misrepresentation, unjust enrichment, and violation of state laws that prohibit "unfair or deceptive" practices.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Of the data protection laws with a private right of action, some require an individual to demonstrate actual injury in order to recover damages, while others, such as BIPA, the CCPA, and the TCPA, award statutory damages to an individual who is the subject of a business' violation of the statute even in the absence of any showing of injury. Of the laws that require a showing of injury, courts are divided as to the nature of the injury required. Courts generally require harm to go beyond mental distress, embarrassment, or inconvenience, without more. Individuals that have been able to point to monetary damage (as opposed to less tangible forms of injury such as emotional harm, lost time, or a loss of privacy) have been more successful in bringing their claims.

In addition, U.S. courts frequently require individuals to establish "standing," that is, an injury sufficient to give them a personal stake in the case such that the court can render a decision. Often, this is a lower bar than what is required to actually establish a right to recover. For instance, facing a "risk of harm" can sometimes be enough to afford a plaintiff standing, but it is typically insufficient to satisfy the injury element of a claim, if any. Courts are also divided on whether and when a plaintiff subject to a violation of a statute is sufficient injury in and of itself to give the individual standing.

43. How are data protection laws in your jurisdiction enforced?

Federal and state data protection laws are enforced at the federal and state levels, respectively. The FTC generally handles enforcement at the federal level, although other agencies or state attorneys general may also enforce certain laws: for example, HIPAA is enforced by the federal HHS and state attorneys general. The FTC may pursue companies for violations of particular U.S. data protection laws and has claimed authority to bring enforcement actions over the data protection practices of all companies under its jurisdiction via Section 5 of the FTC Act (prohibiting deceptive or unfair practices in or affected commerce). When the FTC proceeds under the FTC Act for a first-time violation, it may generally obtain only an injunction or order to cease and desist. If certain requirements are met, the FTC may also obtain disgorgement or restitution. The FTC cannot impose

penalties for first-time violations of Section 5 but can do so for violation of certain of the sector-specific privacy statutes it enforces. A business that violates an order or injunction that resulted from an FTC action is subject to civil penalties or sanction for contempt of court.

At the state level, enforcement of data protection laws typically fall to state attorneys general. In Colorado, district attorneys are concurrently empowered to enforce the CPA. There is substantial variation in enforcement power and actions among the different state regulators. In addition, the new enforcement body in California, the CPPA, began enforcing the CCPA on February 9, 2024, after an appeals court overturned a lower court order enjoining enforcement.

Generally speaking, most enforcement actions and settlements are made public. For example, the California Department of Justice has a privacy-related enforcement actions page, and the Connecticut Attorney General recently issued a report overviewing the first six months of enforcement of the CTDPA. Other state privacy laws set out the range of penalties that may be issued and may also provide for equitable remedies, such as an injunction. Fines at the state level are usually issued on a per-violation basis.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

Below is a summary of the penalties set forth in several key federal data protection laws:

- FCRA: Damages for willful violations by the consumer reporting agency, information furnisher or entity using the information are either actual damages or statutory damages between $100 and $1,000 per violation and can include punitive damages and attorneys' fees and costs, as decided by the court. Damages for negligent violations include actual damages and attorneys' fees and costs.
- HIPAA: Penalties depend upon a number of case-specific circumstances, including the covered entity or business associate's "state of mind" and any aggravating or mitigating factors. Fines are issued in four tiers based on the entity's level of culpability: (1) when the entity had no knowledge (and by exercising reasonable diligence, would not have known) a minimum of $137 per violation, up to $68,928; (2) the violation was due to reasonable cause, a minimum of $1,379 per violation, up to $68,928; (3) the violation was due to willful neglect but corrected within 30 days, a minimum of $13,785 per violation, up to $68,928; and (4) the violation was due to willful neglect and not corrected within 30 days, a minimum of $68,928 per violation, up to $2,067,813. Fines are generally issued on a per-violation basis, per calendar year that the violation occurred. The maximum fine per violation in a calendar year is $2,067,813. State attorneys general may also enforce HIPAA and can issue fines up to $25,000 per violation per calendar year. HIPAA violations may also carry criminal penalties.
- COPPA: The FTC's COPPA Rule implementing the federal law empowers the FTC to seek civil penalties of $51,744 per violation, generally, for *each* child whose personal information was collected in violation of the statute, in addition to nonmonetary injunctive relief. In practice, however, penalty amounts are generally determined by a number of factors, including the egregiousness of the violations, whether the entity has previously violated the statute and the number of children affected. State attorneys general enforcing COPPA violations generally do so under the state's unfair and deceptive trade practices act, which provides for lower penalty amounts.
- GLBA: Financial institutions that offer financial products or services such as loans, financial or investment advice or insurance are required to share their information sharing practices to their consumers and safeguard their sensitive data. Under the GLBA, financial institutions face fines up to $100,000 for each violation and individuals in charge may be found individually liable for up to $10,000 for each violation and face up to five years in prison.

Typically, U.S. state privacy laws grant state attorneys general the authority to initiate an enforcement action for injunctive relief or civil penalties. Most states permit civil penalties of up to $7,500 per violation, though this ranges from $2,500 (*e.g.*, California) to $20,000 (*e.g.*, Colorado). When the FDBR comes into effect, it will permit penalties of up to $50,000, which may be trebled in certain circumstances, although the narrow scope of the law will render few businesses subject to the high penalties. Some states differentiate between penalties for negligent and intentional violations, and California permits higher penalties for violations involving children.

In the two states that have enacted specific consumer

health privacy laws (Washington and Nevada), a violation of either law is considered an unfair and deceptive act, punishable by the penalties permitted by the respective state consumer protection act. The Washington Attorney General may recover a civil penalty of $7,500, actual damages, or in some cases, treble damages of up to $25,000. The Nevada Attorney General may recover a civil penalty of up to $10,000 per violation.

As discussed above, all 50 states have unique personal data breach notification laws that require businesses to notify consumers and / or regulators if the personal data they process is involved in a breach. Penalties and violations vary by state. Some states, such as Michigan, have maximum penalties per breach (with a $750,000 maximum), while other states, such as New Jersey, allow for penalties to be made up of a combination of civil penalties, substantial fines to the state, and investigative costs where penalty ceilings do not exist.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

The rules regarding the calculation of fines are typically outlined within the laws themselves, and recent enforcement actions may provide additional insight into the factors weighing into the regulator's decision.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Yes, orders issued by regulators, such as the FTC, may generally be appealed to a court of appeal.

If the court of appeal upholds the regulator's decision, then the controller may file a request for the Supreme Court to review the case, which the Supreme Court may grant or deny.

The court of appeal and, if applicable, the Supreme Court may in some situations defer to the findings of the regulator.

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

Regulators and state attorneys general have become increasingly active in enforcing data protection laws and have taken a number of actions to hold companies accountable for violations.

The California Attorney General has made public examples of enforcement cases that make clear themes of focus, including failure to honor opt-outs; noncompliant or missing privacy notices; failure to honor individual rights requests; noncompliant service provider contracts; untimely responses to requests; charging fees for fulfilling CCPA requests; and failing to provide consumers a mechanism by which to exercise their rights. The California Attorney General also conducts periodic "investigative sweeps" of businesses subject to the CCPA, and most recently has focused on streaming services' compliance with opt-out requirements. Moreover, following an appeals court's recent decision to overturn a lower court injunction, the CPPA will likely soon pick up such enforcement activity.

The Connecticut Attorney General released in February 2024 a report on enforcement actions it has taken under the CTDPA since the law came into effect. The report reveals the Connecticut Attorney General's focus on insufficient privacy notices and rights mechanisms. The report also identifies sensitive personal data, children and teenager personal data, and data brokers as other areas of enforcer interest.

The FTC has increased its enforcement in the health privacy space. In addition to issuing recent guidance about healthcare privacy, in 2023 the FTC issued three major enforcement actions regarding health data. Relatedly, the FTC has indicated its interest in the sale of precise geolocation data that may reveal health information about consumers: in 2023, the FTC issued three enforcement actions regarding the inappropriate sale of precise geolocation data.

In addition, regulators have started targeting companies that fail to adequately communicate with investors or affected consumers regarding material data breaches. For example, the FTC alleged unfair and deceptive practices against a software provider that allegedly made delayed and misleading notification of a data breach to its customers, deceptive security statements, and unfair data retention practices and information security practices. Similarly, the software provider settled with the SEC in connection with allegations that the business had made materially misleading statements regarding the data breach in its security filings.

U.S. regulators are clearly increasingly active in enforcing data protection laws. Business should ensure that they are complying with all applicable data protection laws to avoid facing penalties and other enforcement actions.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

The number of comprehensive privacy laws enacted by U.S. states has continued to rise in the past year. Seventeen states are actively considering comprehensive consumer data privacy bills; in addition to the five states that have comprehensive privacy laws already in effect, another ten states (Delaware, Florida, Indiana, Iowa, New Hampshire, New Jersey, Oregon, Montana, Tennessee, Texas) have enacted laws that will come into effect in 2024 or thereafter. The Kentucky legislature has passed a comprehensive privacy bill that, as of the time of writing, is awaiting the governor's signature. Despite significant developments at the state level, there remains no general federal privacy bill likely to be signed into law at this time.

Children's online safety laws continue to be of great interest to legislators. In the federal legislature, Congress is considering four major reforms: the Kids Online Safety Act ("KOSA"), the Children and Teens' Online Privacy Protection Act ("COPPA 2.0"), Strengthening Transparency and Obligation to Protect Children Suffering from Abuse and Mistreatment Act ("STOP CSAM Act"), and Eliminating Abusive and Rampant Neglect of Interactive Technologies Act ("EARN IT Act"). While it is still unclear which, if any, of these bills will pass into law, Congress has demonstrated a clear interest in regulating the online safety space.

Meanwhile, lawmakers across the country are also attempting online safety reforms at the state level. Many of these bills require reasonable age verification mechanisms, data protection impact assessments, and restrictions on targeted advertising, the sale of data, profiling, data minimization, and the collection of precise geolocation data. Hawaii, Illinois, Kentucky, Maryland, Minnesota, New Jersey, Pennsylvania, South Carolina, Vermont, and Virginia are considering age-appropriate design codes that draw on California's equivalent and require controllers to use reasonable care to mitigate the heightened risk of harm to minors proximately caused by using their service.

Colorado, Kentucky, Missouri, Nebraska, New York, and Vermont have all introduced or reintroduced bills that seek to mimic Illinois' BIPA, while the Illinois legislature has proposed amendments to BIPA itself, including as they relate to consent requirements, a new cure period, and limiting the recovery of statutory damages.
In the health data space, many bills have been introduced (Hawaii's HB1566, Illinois' SB3080, and Vermont's S173) that track Washington's MHMD Act, which was designed to protect health data that is not otherwise covered by HIPAA, bringing under its scope businesses that are not covered entities under HIPAA and that process health data. The New York Senate also recently passed S158B, which would introduce strict consent and necessity requirements for processing of health data.

Increasingly, states are proposing legislation surrounding AI. For example, California's AB2930 would regulate developers and deployers of automated decision-making tools and require impact assessments, consumer notification, and corresponding opt-out rights. Connecticut's SB2 would regulate "high-risk AI systems" and generative AI, including transparency requirements and protections against algorithmic discrimination. New York's S8755 would create an AI ethics commission to oversee use of AI within New York state agencies and private entities operating within the state. Similar bills in Illinois, Oklahoma, Rhode Island, Virginia, and Vermont are under consideration.

The federal government has also indicated a strong interest in regulating AI: Congress is considering a number of AI-related laws that would require labeling of AI-generated content, create remedies for individuals impacted by deepfakes, prohibit collusive pricing algorithms, and restrict the use of automated decision-making systems by employers, among other items. In October 2023, U.S. President Joe Biden issued an executive order outlining AI policy principles and requirements for federal agencies. The principles from the executive order are likely to influence future regulation of both the public and private sectors' use of AI.

Contributors

Heather Egan
Partner
hegan@orrick.com

Sulina Gabale
Partner
sgabale@orrick.com

Thora Johnson
Partner
thora.johnson@orrick.com

Emily S. Tabatabai
Partner
etabatabai@orrick.com

Shannon Yavorsky
Partner
syavorsky@orrick.com

Bianca Giulia Ponziani
Managing Associate
bponziani@orrick.com