COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

United States

DATA PROTECTION & CYBER SECURITY LAW

Contributor

Orrick, Herrington & Sutcliffe LLP

Heather Sussman

Partner | hsussman@orrick.com

Sulina Gabale

Partner | sgabale@orrick.com

Thora Johnson

Partner | thora.johnson@orrick.com

Tori Downey

Associate | tori.downey@orrick.com

Kathryn Boyle

Associate | kboyle@orrick.com

Oladoyin Olanrewaju

Associate | oolanrewaju@orrick.com

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

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

UNITED STATES
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy 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). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

There is no single, omnibus U.S. federal law addressing data privacy rights and obligations. Federal laws, which apply to residents in all states, are generally sector-specific and primarily regulate the financial and healthcare sectors, the telecom industry, government contractors and children. State laws, where they exist, more frequently look to protect consumers residing in that state, which is permitted under the U.S. system that allows states to regulate absent federal preemption or an undue burden on interstate commerce.

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 Information 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 age 13 and requires related privacy notices and in many instances verified parental consent; and the Family Educational Rights and Privacy Act (FERPA), which regulates privacy of student records.

Moreover, federal laws, such as the Telephone Consumer Protection Act (TCPA) and the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act, also regulate calling 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 and unfair practices in or affecting commerce, including to require companies to disclose unexpected data practices prior to collection, to enforce failures to comply with published privacy policies and to require companies to reasonably protect personal information in their custody or under their control.

Many states also have laws that protect the personally identifiable information of residents, but the level of protection and the types of information considered to be personally identifiable differ from state to state. To varying extents, state laws commonly restrict the information that may be collected during retail or credit card transactions, limit the recording of communications without consent, and protect minors.

Some states are more protective of privacy than others. Massachusetts, for example, has data protection 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, imposing cybersecurity requirements on all covered entities and applicable third parties. California (Cal. Civ. Code §§ 1798.83-84, 1798.100 et seq.; Cal. Bus. & Prof. Code §§ 22575-82; Cal. Ed. Code § 99122), Connecticut (Conn. Gen. Stat. § 42-471), Delaware (Del. Code Tit. 6 § 1201C et seq.), Pennsylvania (18 Pa. C.S.A. § 4107), Nebraska (Neb. Stat. § 87-302), Nevada (NRS § 603A.300 et seq.), Oregon (ORS § 646.607) and Utah (Utah Code §§ 13-37-201 to -203) are all examples of states that have laws regarding privacy policies. Many states restrict 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 providing greater levels of student privacy than are accorded under FERPA. Around a dozen states have their own, often more restrictive version, of the VPPA. States also regulate the use and protection of personal information by insurers.

Among the states, California has been especially protective of consumer privacy. Currently, there are limited protections under California's Shine the Light law and the California Online Privacy Protection Act (CalOPPA), which Nevada and Delaware have copied in large part; but broader, more European-style data subject rights took effect on January 1, 2020, under the California Consumer Privacy Act (CCPA), which mandates that California residents have data access and portability rights, data deletion rights, and the right to request that personal information not be sold, with "sale" broadly defined 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' practices regarding their own personal information upon verified request. In addition, companies may not discriminate against California consumers who exercise their CCPA rights. In the November 2020 statewide election, the California Privacy Rights Act (CPRA) was passed by a majority vote. The CPRA proposes a number of revisions to the CCPA, addressing ambiguities and overly burdensome requirements, while simultaneously introducing new privacy and security obligations for covered businesses. For example, the CPRA will revise and expand the scope of covered "businesses" under the CCPA, add a second category of personal information ("sensitive personal information"), broaden the notice at collection, adopt an explicit overarching purpose-limitation obligation, and add new consumer rights and revise existing obligations. The CPRA becomes fully operative on January 1, 2023 and will be enforced by the new California Privacy Protection Agency beginning on July 1, 2023.

Following California, Virginia, Colorado and Utah enacted comprehensive consumer data protection legislation. The Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (CPA) and the Utah Consumer Privacy Act (UCPA) will become effective on January 1, 2023, July 1, 2023 and December 31, 2023, respectively. Each law will impose new obligations on both controllers and processors with respect to personal data of consumers, and grant new rights to consumers with respect to their personal data, among other obligations.

In April 2022, the Virginia Governor signed into law amendments to the VCDPA. The amendments add a new exemption to the legislation's right to delete; shift all civil penalties, expenses, and attorney fees collected pursuant to the law into the state treasury to be credits to the existing Regulatory, Consumer Advocacy, Litigation, and Enforcement Revolving Trust Fund (replacing the originally proposed Consumer Privacy Fund); and expand the definition of "nonprofit organization" to include "political organizations."

All states have data security and breach notification laws, though the scope of what data is covered as well as the 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 registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

The U.S. does not have any privacy-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 a 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 selfregulatory 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.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

Because there is no single, overarching privacy law in the U.S., there is no one concept of personal data or personally identifiable information. In general, all U.S. privacy laws protect some form of "personal data," "personal information (PI)," or "personally identifiable information" (PII), but the scope of coverage varies significantly. Some of these laws may also have special designations for sensitive information, such as health information, and Social Security numbers (SSNs) or individuals' tax identification numbers, requiring additional disclosures or protections before that data can be collected or processed. PII generally refers to information used to distinguish or trace an individual's identity, such as name, SSN, date of birth, mother's maiden name or biometric records, or any other information that is linked or linkable to an individual.

For data breach notification purposes, the definition of "personal information" is usually laid out in each state's data breach notification law and may vary by state. However, most breach notification laws define personal information as an individual's name plus:

- SSN;
- driver's license number; or
- financial account number, if paired with sufficient information to access funds in the account.

Increasingly, states are amending their state breach notification laws to add medical information or health insurance number and username and password to the definition of personal information. Breach of this information would require notification to the impacted consumer.

Other definitions of "personal information" or "personal data" under federal law include:

- personal information of children under 13, broadly defined under COPPA;
- protected health information (PHI), defined in HIPAA; • nonpublic personal information, defined in GLBA; and
- consumer credit and other information, defined in FCRA.

State definitions of PII and PI vary as well. The California Attorney General, for example, has stated that mobile device identifiers are PI. Additionally, California's privacy laws set out their own definitions of "personal information." For example, California's Shine the Light law identifies 27 categories of personal information, including – in addition to common PII categories – the number, age and gender of children; political party affiliation; products purchased, leased or rented by a consumer; real property purchased, leased or rented; payment history; and type of service provided. 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 specifically includes 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. Under the CCPA, there are 11 categories of personal information, and these categories must be used when providing required notices of purposes of collection, use and disclosure. The CPRA will create a second category of personal information, "sensitive personal information," with additional compliance requirements (described in greater detail below). Under the CPRA, the definition of sensitive personal information includes but is not limited to: 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, biometric data, and personal information collected and analyzed concerning a consumer's health.

In Virginia, Colorado and Utah, the VCDPA, CPA and UCPA define "personal data" as "any information that is linked or reasonably linkable to an identified or identifiable natural person", and does not include de-identified data or publicly available information. Similar to the CPRA, the VCDPA, CPA and UCPA will further provide a separate category for "sensitive data," defined as "a category of personal data that includes (i) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (ii) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; or (iii) the personal data collected from a known child;." The VCDPA and UCPA also include precise geolocation data in their definition of "sensitive data."

Under New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, the definition of "private information" has been broadened to include biometric information, and username or email address in combination with a password or security questions and answers that would permit access to an online account. It also includes an account number, or credit or debit card number, wherein the circumstances permit access to an individual's financial account without additional identifying information, security code, access code or password.

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

In general, privacy laws in the U.S. do not expressly impose specific principles related to the processing of personal information. Accordingly, there is no uniform view of how personal information should be processed.

Similar to the Organisation for Economic Cooperation and Development's (OECD) Fair Information Practices, however, the FTC has promulgated fair information practice principles (FIPPs) for the way in which online entities collect and use personal information and safeguards to assure that practices are fair and provide adequate information security. The "core" principles are: (i) Notice/Awareness; (ii) Choice/Consent; (iii) Access/Participation; (iv) Integrity/Security; and (v) Enforcement/Redress. (The last principle, Enforcement/Redress, was removed in the FTC's 2000 report to Congress.)

Under the notice principle, consumers are expected to be made aware of an entity's data practices prior to collection of their personal information. Without providing prior notice, informed consent to data collection and disclosure cannot be given. Additionally, three of the other principles (choice/consent, access/participation and enforcement/redress) are meaningful only when a consumer has been given notice of an entity's practices and their rights with respect to the entity's data practices.

The choice/consent principle refers to consumer choice or consent. Choice means providing consumers options as to how and whether their personal information is collected, how it is used, and whether any secondary uses of information (i.e., uses beyond those they consented to or are necessary to complete the contemplated transaction) are permitted.

Access/participation relates to a consumer's ability to view the data that an entity has collected, used or disclosed, as well as the ability to correct inaccurate or incomplete data. Under this principle, businesses should provide a mechanism for consumers to access or correct their data that is inexpensive and timely.

The integrity/security principle goes along with the above principle. Data integrity requires the data an entity processes about a consumer to be accurate and secure. This requires entities to take reasonable steps to ensure the data is accurate, such as using reputable data sources and providing consumer access to data.

Lastly, enforcement/redress provides a means to ensure the principles are actually effective. Absent an enforcement and redress mechanism, the incentive for an entity to institute or comply with policies and procedures that align with the principles is likely to be lost.

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

The principles, however, underlie both federal and state laws, and continue to serve as a model for data privacy protections in developing areas and industries. For

example, in California, the recently passed CPRA will impose an explicit, overarching purpose limitation principle, codifying a key concept found in the FIPPs, 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." Additionally, the VCDPA in Virginia will impose both a collection limitation and purpose limitation upon controllers, requiring controllers to obtain the consumer's consent for processing personal data for a purpose neither reasonably necessary nor compatible with the disclosed purposes for which such personal data is processed absent an exception. Colorado also creates several specific processing duties for controllers under the CPA including transparency, purpose specification, data minimization, avoiding secondary use, a duty of care, avoiding unlawful discrimination and the protection of sensitive data.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

There is no single federal law in the U.S. that sets out general requirements for when and how to obtain consent from data subjects. Instead, consent requirements are regulated by various individual sector-specific laws. In particular, in the U.S., certain types of information require opt-in consent. These include health information, credit reports, financial information, student data, personal information collected online from children, biometric data, video viewing choices, certain uses of phone numbers, and geolocation data. Certain other uses of personal information are subject to opt-out consent (e.g., email marketing, or in California the "sale" of PI), and the rest are generally not subject to any consent requirement at all.

The U.S. regulates the type of consent an entity must obtain prior to communicating with an individual directly via email, phone, text or fax. Specifically, under the TCPA, in many circumstances consent must be obtained from the recipient of a call or text before a call is placed or a text is sent, particularly in the context of marketing. Whether and what kind of consent must be obtained (for example, none vs. "prior express consent" vs. "prior express written consent") depends on the type of call (emergency, sales/marketing, transactional/informational); the type of calling technology used (manual dial, auto-dialer, prerecorded voice); the type of phone called (residential landline, cell phone); the type of caller (for-profit, nonprofit, state/local government, federal government); and the type of recipient of the call (business-to-consumer vs. business-tobusiness).

With regard to biometric data, certain states require specific kinds of consent before collection. In particular, the Illinois Biometric Information Privacy Act (BIPA) requires that written consent be obtained before collecting a biometric identifier.

In addition, under the FTC Act, companies generally need to obtain opt-in consent prior to using, disclosing or otherwise treating PII in a manner that is materially different from what was disclosed in the privacy policy applicable when the PII or PI was collected.

6. 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 content and administration of such consent depends upon the applicable law, and at times, the purpose(s) for which the 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 freely given by an individual, unambiguous, specific and informed.

States have been following the trend to legislate against dark patterns, which mean a user interface designed or manipulated with the substantial effect of subverting or impairing autonomy, decision-making or choice. For example, both the CPRA and CPA specify that consent is not valid if obtained through "dark patterns."

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

In general, privacy laws in the U.S. do not designate specific categories of personal information as sensitive. Accordingly, there is no uniform view of what constitutes sensitive personal information in the U.S., although certain types of data, such as financial and health

information, and PI collected online from children, or by schools or their contractors from or about students, often are subject to heightened protections. For example, HIPAA imposes privacy and security obligations on entities that handle PHI; GLBA protects "nonpublic personal information" maintained by financial institutions about their customers; FCRA governs how consumer reporting agencies collect, use and disclose consumer credit information; and the Genetic Information Nondiscrimination Act prohibits certain uses of genetic information. There also are state laws applicable to particular categories of personal information that may be considered sensitive, such as laws concerning the collection, use and retention of biometric information (for example, the Illinois BIPA) and requiring heightened data security safeguards for regulated financial institutions and insurers (for example, the NYDFS Cybersecurity Regulation). New York also differentiates between "personal information" and "private information," with private information being a more sensitive subset of personal information, which includes biometric information or financial account information that does not require a security code for access. Relatedly, certain federal and state nondiscrimination laws prohibit soliciting certain types of personal information or using such information to the detriment of a protected class or group, particularly in housing, employment and credit. California's Unruh Civil Rights Act prohibits discrimination in public accommodations, or the offering of products or services, based on any of a large 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.

Once fully operative on January 1, 2023, the CPRA will require covered businesses to provide separate disclosures for sensitive personal information collected, including the purpose for its collection and use, and whether the sensitive personal information is sold or shared. Covered businesses will be prohibited from collecting additional categories of sensitive personal information or using sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected, without first providing the consumer with notice. The CPRA will also create a new right for consumers – the Right to Limit Use and Disclosure of Sensitive Personal information – which, absent an exception, grants consumers a right to direct a business to limit its use of the consumer's sensitive personal information, and requires businesses to create a "Limit the Use of My Sensitive Personal Information" link on its online services. Under both the VCDPA and the CPA, controllers will be prohibited from processing sensitive data without first obtaining the consumer's consent. The UCPA will prohibit controllers from processing sensitive data without first presenting consumers with clear notice and the opportunity to opt out of the processing.

8. How do the laws in your jurisdiction address children's personal data or PII?

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 collection, use or disclosure of children's personal information, 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 addition, FERPA governs how schools collect, use and disclose personal information from a student's educational record, and applies to all schools that accept federal educational funding, including Kindergarten-12 as well as institutions of higher education. FERPA sets forth certain rights and restrictions concerning the disclosure of students' educational information – which generally requires written consent of the student, or if the student is under 18, written consent of the parent or legal guardian – and how parents and students may access, correct or delete student educational information.

A handful of states have implemented privacy laws that specifically address the collection and use of children's, students' or minors' personal information. For example, 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. Michigan and Utah have Child Protection Registry Acts. And nearly every state has laws governing schools' and third-party contractors' collection, use, disclosure and sale of

student data collected or generated in connection with educational technology or services in a school setting. In addition, under the CCPA (and, once fully operative on January 1, 2023, the CPRA), businesses may not sell PI of California residents under the age of 16 without the minor or, in the case of children under 13, their parent's, opt-in consent. Once effective on January 1, 2023, Virginia's CDPA will require controllers to process sensitive data concerning a known child in accordance with COPPA. Once effective on December 31, 2023, the UCPA will be similar in this regard to the VCDPA. The CPA, once effective on July 1, 2023, will prohibit controllers from processing personal data concerning a known child without first obtaining consent from the parent or lawful guardian.

9. Does the law include any derogations, exclusions or limitations other than those already described? 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 and GLBA. In some cases, state privacy laws have carve-outs for entities or individuals subject to sector-specific federal laws. For example, California's CCPA has exclusions of various degrees for data governed by HIPAA, GLBA, FCRA, and other state and federal laws. The CPRA, VCDPA, CPA and UCPA will have similar carve-outs once operative and/or effective in 2023.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

The U.S. generally does not impose requirements of data protection by design or default. However, the CPRA, VCDPA, CPA and UCPA will impose purpose and/or collection limitations on covered entities, codifying aspects of the FIPPs and Europe's General Data Protection Regulation (GDPR) Article 25 data protection by design and by default principles. For example, the CPRA and VCDPA will 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 and CPA will also limit 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.

Generally, however, the FTC has recommended that companies consider both privacy and data security when designing and developing their products and services. In cases where a company 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.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Owners or processors of PII or PI are not generally required to maintain any internal records of their data processing activities or to establish internal processes or written documentation.

However, there are several statutory frameworks in the U.S., including GLBA, HIPAA, and some state information security and health laws, that require specific record retention practices as well as the implementation of associated information security programs. These programs typically require internal processes and documentation of the administrative, technical and physical safeguards implemented to protect the confidentiality and security of personal information. In turn, certain of these regulations subsequently require documentation of those practices. For example, HIPAA requires covered entities to maintain related documentation for six years from date of creation or when last in effect, whichever is later. Finally, entities also typically use industry or third-party benchmarking data to determine how best to maintain records generally, including data processing documentation. Creating and maintain data processing inventories can aid in compliance efforts when required to disclose how a business collects, uses or discloses personal information, as well as the sources or recipients of the personal information, under states laws such as the CCPA, CalOPPA, Nevada Senate Bill 220 or the Delaware Online Privacy and Protection Act (DOPPA), and, once fully operative and/or effective in 2023, the CPRA, VCDPA, CPA and UCPA.

12. Do the laws in your jurisdiction require

or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

and disposal. 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 there are no HIPAA retention requirements for medical records, HIPAA provides that covered entities must record any policies, procedures, actions or assessment carried out to comply with HIPAA for a minimum of six years after their creation or, if the document outlined a policy, six years from when the policy was last implemented. 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.

There are also state laws that obligate businesses to retain certain data for specific periods of time. For example, the CCPA (and once fully effective in 2023, the CPRA) 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.

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

Consultations with regulators regarding privacy and data security matters are not generally required in the U.S., 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 the underlying purpose of the consultation is focused on other issues. Although not formally recommended in most cases, it may be advisable to consult with a regulator under certain circumstances.

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

While periodic risk assessments are often advisable, data security risk assessments are currently explicitly required only for certain industries in a limited number of jurisdictions. For example, New York requires regulated financial institutions and insurers to conduct a risk assessment and then implement an information security program based on the assessment (under the NYDFS Cybersecurity Regulation). Similarly, the FTC amended the GLBA Safeguards Rule (effective January 10, 2022) to require financial institutions to institute as part of their security program continuous monitoring or period penetration testing and vulnerability assessments. Tabletop exercises can assist a business handling sensitive personal information to train personnel and to determine weak spots in data security policies and systems. Privacy impact assessments have not been mandated by law in the U.S. as they have in other countries. However, the FTC and many state attorneys general have advised adoption of privacy-by-design and use of privacy impact assessments as a best practice.

Once fully operative and/or effective in 2023, the CPRA, the VCDPA and the CPA will require a form of a risk assessment. In particular, both the VCDPA and the CPA will require controllers to conduct and document a data protection assessment for the processing of personal data for purposes of targeted advertising, the sale of personal data, the processing of personal data for purposes of profiling that presents certain reasonably foreseeable risks to the consumer, the processing of sensitive data, and any processing activities involving personal data that present a heightened risk of harm to consumers. The CPRA calls for regulatory requirements for annual risk assessments and cybersecurity audits for companies whose processing of personal information presents a significant risk to consumers' privacy or security. The statute provides that the forthcoming regulations should consider the size and complexity of the business and the nature and scope of processing activities when determining the criteria for applicability. Any CPRA-required risk assessments will need to include whether the business' processing involves sensitive personal information, and identify and weigh the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the risks to the rights of the consumer associated with such processing. The CPRA's risk assessment requirement evokes the GDPR concept of

the data protection impact assessment but goes further by requiring such assessments to be submitted to a regulatory body, the California Privacy Protection Agency, on a regular basis. The CPRA, VCDPA and CPA stand in contrast to the UCPA, which at this time will not require companies to conduct risk assessments.

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) 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 company hire a chief privacy officer who has C-level authority with direct reporting to the chief executive 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. HIPAA considers a covered entity to be any health plan, healthcare clearinghouse or healthcare provider in the U.S. that transmits health information in electronic form. HIPAA considers a business associate to be any person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. The privacy and security officer(s) can have other titles and duties in addition to these roles. The privacy officer is responsible for overseeing the organisation's development, implementation and maintenance of HIPAA-compliant privacy policies and procedures for all health information, not just that which is stored or transmitted electronically. 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 their staff are properly trained on the applicable HIPAA requirements.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

There are a number of U.S. federal and state statutes that explicitly require employee training. For example, the HIPAA Privacy Rule requires covered entities to train all members of its workforce as necessary and appropriate in order for the members of the workforce to carry out their functions. In addition, the 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 such as that of the now-required "qualified individual" responsible for overseeing and implementing a financial institution's information security program and enforcing their information security program.

Similarly, PCI-DSS requires that entities educate employees immediately after hire and at least annually. Entities must also implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. The security awareness program also requires that staff with security breach response responsibilities are periodically trained.

The CCPA (and once fully effective on January 1, 2023, the CPRA) require 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.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

There is no omnibus federal law that requires entities to provide notice to individuals when collecting, processing or disclosing personal information. However, the FTC, which serves as the closest thing the U.S. has to a lead data protection authority, takes the position that under Section 5 of the FTC Act (which prohibits deceptive or unfair acts or practices in or affecting commerce), it is an unfair business practice not to disclose material data practices, especially if they would be unexpected, and that any material omissions or inaccuracies in privacy notices are a deceptive practice. In addition, several federal sector-specific laws require privacy notices. For example, HIPAA requires covered entities to provide a health information privacy notice titled "Notice of Privacy Practices" and obtain consent prior to certain types of disclosures of PHI; GLBA requires financial institutions to provide annual privacy notices and certain privacy choices; the Cable Communications Policy Act requires notice and consent for cable communications providers to disclose subscriber information except to the extent necessary to render core cable services; and COPPA requires online service operators to post a privacy notice for parents to read, and further requires various levels of consent prior to collection of personal

information from children. Most states have their own versions of HIPAA and GLBA that can set higher standards, and 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 providers, some of which include privacy notice obligations.

Certain states have laws requiring privacy notices with broader applicability, depending on the circumstances, including California, Nevada, Delaware and Connecticut. For example, businessto-business entities are required to post a privacy policy consistent with Delaware law, while California and Nevada merely regulate consumer transactions and solicitations. California has the most robust privacy notice laws, including CalOPPA, which requires online consumer services to post a privacy policy; the California Shine the Light Law, which requires entities to post a privacy policy (online or offline) disclosing whether they share consumer personal information with third parties for the third parties' own direct marketing purposes; California's Privacy Rights for California Minors in the Digital World law, which requires a disclosure describing how a minor under age 18 can delete publicly available personal information they have submitted online; and the CCPA, which requires notice prior to collection, robust privacy policy disclosures, and businesses to provide California consumers with certain rights over the access to and control of personal information. Once fully operative and/or effective in 2023, the CPRA, VCDPA, CPA and UPCA will require a covered organisation to provide consumers with a reasonably accessible, clear and meaningful privacy notice about the organisation's privacy practices and consumer rights.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

Currently, U.S. privacy laws generally do not apply directly to service providers, and most requirements stem from flow-down data owner contractual requirements. There are, however, several sector-specific federal laws, such as HIPAA, GLBA, FCRA, and COPPA, that may require certain service provider activities and apply related standards. 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 of, misuse of, unauthorised access to or modification of information.

The CCPA regulates service providers and has complex provisions regarding when making PI available to a vendor is or is not a sale subject to a "do not sell" request and when the business and the service provider are or are not entitled to a safe harbor as to the other's noncompliance with the law. Businesses should contract effectively relative to service providers to establish the scope of permissible uses of personal information and the service provider designation, as well as to develop a mechanism for flow-down obligations with consumer access and deletion requests. Once fully operative on January 1, 2023, the CPRA will further expand service provider contractual obligations and flow down obligations. The CPRA will create an overarching contracting requirement for businesses that sell, share or disclose for a business purpose the personal information of a consumer to a third party, service provider or "contractor" to enter into an agreement with specific contracting obligations. Although the CCPA already imposes contract obligations on service providers and the newly relabeled "contractors," imposing contracting obligations with third parties will significantly increase the scope and flow-down impact of the CPRA on business transactions. Further, the CPRA will obligate not only businesses, but in some cases, service providers and contractors, to pass consumer rights requests downstream to other parties who accessed the consumer's personal information.

Additionally, similar to Europe's GDPR, the VCDPA, CPA and UCPA distinguish between controllers and processors, and provide affirmative obligations not only on the controller, but also on the processor. For example, under the VCDPA and CPA, processors will be required to comply with the controller's instructions, to enter into the necessary contracts with the controller, and to assist the controller in meetings its obligations under the VCDPA and CPA, including in relation to (i) consumer rights requests, (ii) protecting personal data and reporting any breach of personal data, and (iii) data protection assessments.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of

processors (e.g., due diligence or privacy and security assessments)?

Currently, most U.S. privacy laws generally do not require minimum contract terms with service providers. However, there are several sector-specific federal laws, such as HIPAA, GLBA, FCRA, FERPA and COPPA, that may require service providers to be retained and governed by written agreements with specific provisions, and the CCPA also takes this approach. Many state laws highly recommend that a written information security plan be included as part of the contractual requirements for service providers. In addition, California and Massachusetts laws require nonaffiliated service providers to contractually agree to take reasonable and appropriate measures to protect shared personal information, and Connecticut law requires contractors working with the state to encrypt all sensitive personal data that is transmitted wirelessly or via public internet connection or is visible on portable electronic devices. Some states also look to the PCI-DSS as the de facto benchmark for determining whether a service provider is sufficiently secure in the relevant context.

The CPRA, the VCDPA, the CPA and the UCPA expand contracting obligations on covered entities. For example, the CPRA creates an overarching contract requirement for businesses that sell, share or disclose for a business purpose the personal information of a consumer to a third party, service provider or "contractor" to enter into an agreement; it also creates a new "contractor" label and contract specifications, new service provider contract specifications, and significantly increases the scope and flow-down impact on businesses transactions by requiring businesses to enter into contracts with third parties. Similarly, the VCDPA, CPA and UCPA require controllers to enter into a contract with any processor, which among other things, sets forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. Processors also are obligated to enter into the necessary contract with the controllers.

In the educational context, many of the state student data privacy laws require specific contractual provisions to be in place in contracts between educational institutions and their service providers. For example, under California's state student data privacy protection 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.

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

Laws in the U.S. that apply to monitoring, automated decision-making or profiling generally have not historically restricted these activities, but rather regulate or require disclosures regarding the use of cookies and other tracking technologies. While the CCPA is silent about profiling and automated decision-making, the CPRA, the VCDPA and the CPA grant consumers rights regarding opting out of the processing of their personal data for purposes of profiling and create requirements that impact automated decision-making, including profiling.

There are two federal statutes that, although they do not directly apply to cookies, have been used to enforce activities relating to cookies used for tracking and behavioral advertising. For example, the FTC Act has been used as a basis for regulatory enforcement against entities misrepresenting or failing to disclose tracking cookies. Enforcement actions have also been taken on the basis of the Federal Computer Fraud and Abuse Act (CFAA), and state equivalents, against entities using cookies for behavioral advertising, where the cookie allowed for deep packet inspection. Some states have deceptive practices acts which have been used as a basis for enforcement similar to the federal laws described above. 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 and express consent.

Moreover, certain states have laws that impose disclosure obligations as to the use of and/or disablement of tracking technologies. For example, under CalOPPA, and other state laws that have copied it, there is an obligation for entities to disclose in their online privacy policy whether the website responds to "Do Not Track" signals and whether third parties may collect personal information across time and services using tracking technologies associated with them when a consumer uses the site. Similarly, the CCPA requires businesses in their general online privacy policy (or in a separate California-specific privacy policy) to disclose to whom they share or sell personal information, including data gathered from first- or third-party cookies and other tracking technologies. The CPRA will further expand the consumer's right to opt out to apply to a business'

"sharing" of personal information with a third party for purposes of cross-context behavioral advertising, whether or not for monetary or other valuable consideration. Similarly, once effective, the VCDPA, the CPA and the UCPA will allow consumers to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, and – with the exception of the UCPA – profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

In addition, ECPA, SCA, CFAA, and state law equivalents, as well as tort laws, have been used as a basis for lawsuits against companies utilising keystroke and other tracking features on websites and mobile apps. For example, there has been a recent wave of class action lawsuits brought under California's Invasion of Privacy Act (CIPA) against companies for their use of such technologies. In these cases, generally, the plaintiffs assert (i) a vendor's implementation of covert advanced tracking technologies on a company's website constitutes unlawful recording of the plaintiff's interaction with the website under CIPA and (ii) the company is aiding, agreeing with, employing, or conspiring with the vendor to undertake this unlawful recording activity. There has not been any ruling in the CIPA cases as of the date of publication, but companies that use tracking and session replay technologies typically defend this practice by asserting that their privacy policies sufficiently disclose the use of these technologies.

Finally, the Digital Advertising Alliance and the Network Advertising Initiative 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.

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

The CPRA, VCDPA, CPA and UCPA each provide consumers the right to opt out of the processing of personal data for the purposes of cross-contextual behavioral advertising, also referred to as targeted advertising, subject to certain exceptions.

The CPRA defines cross-contextual behavioral advertising to mean "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 CPRA also provides consumers the right to opt out of "sharing" which includes the sharing of a consumer's personal information by a business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

The VCDPA, CPA and UCPA have nearly identical definitions for targeting advertising, which means displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict the consumer's preferences or interests. Notably, the VCDPA and CPA will require controllers who process personal data for purposes of targeted advertising to conduct and document data protection assessments in certain circumstances.

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

The CCPA, CPRA, VCDPA, CPA and UCPA each address the sale of personal information. 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 information 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 information with a service provider that is necessary to perform a "business purpose." If the business sells consumers' personal information, 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 My Personal Information" must be included on the business's Internet home page, if applicable. Once fully effective on January 1, 2023, the CPRA will expand on the CCPA's existing opt-out right to include both the "sale" and "sharing" of personal information. "Sharing" is defined by the CPRA as 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 will be prohibited from selling or sharing personal information 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

who are less than 13 years old) have affirmatively authorized the sale or sharing. Accordingly, the link posted on a business's homepage will be titled under the CPRA, "Do Not Sell or Share My Personal Information."

Once effective in 2023, the VCDPA, the CPA and the UCPA will similarly require businesses to offer consumers the right to opt out of the sale of their personal information. However, there are slight nuances as to how each law defines "sale." The CPA defines "sale" to mean the exchange of personal data for monetary or other valuable consideration by a controller to a third party. The VCPDA and UCPA, however, drop the "or other valuable consideration" and define "sale" to mean the exchange of personal data for monetary consideration by a controller to a third party.

23. Please describe any 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 U.S., federal and state laws limit and 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 communications, including telemarketing calls, autodialed calls, prerecorded calls and text messages as well as fax communications, are regulated by the TCPA, the Telemarketing Sales Rule and individual state laws. The rules pertaining to such communications differ according to the type of communication at issue, such as marketing versus non-marketing communications.

Email communications are regulated by the federal CAN-SPAM Act, which establishes requirements for sending unsolicited commercial email, including clearly identifying the email as a commercial email, and gives consumers the right to opt out of commercial email, including prompt compliance with any opt-out request. CAN-SPAM preempts state laws, except to the extent they prohibit fraud or deception. In short, TCPA is mostly an opt-in scheme, while CAN-SPAM 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.

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

In the U.S., state laws limit and regulate the way in which companies may process "biometric information." Illinois, Texas and Washington currently all have specific biometric privacy laws. Similar laws have been proposed in Alaska, California, Connecticut, Massachusetts, Montana, New Hampshire and New York in recent years. Additionally, there are a number of U.S. cities that have enacted their own facial recognition laws, such as New York City, Somerville (Massachusetts), and Seattle (Washington).

Illinois' BIPA is uniquely strict. The Washington and Texas laws apply to biometric information that is collected or used for commercial purposes, whereas the Illinois statute applies to any collection or use by a private entity. Additionally, while civil penalties are imposed for violations under all three states' biometric privacy laws, only Illinois' 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, including in the employment context, without consent.

Illinois' 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 generally or subject to HIPAA regulations. 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 "biometric identifier."

There are five main obligations under Illinois' BIPA: (i) an entity 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, an entity must prove 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) an entity must either obtain consent from or be authorized by an individual to

disclose biometric data; (iv) an entity cannot sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information; and (v) reasonable security measures are required for the storage or transmission of biometric data.

As mentioned above, a violation of Illinois' BIPA can result in large 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;
- Reasonable attorneys' fees and costs.

Of note, at the federal level, the FTC has recently increased its focus on unfair and deceptive trade practices in relation to facial recognition technology, going as far as declaring it "discriminatory and dangerous." We can expect that the FTC will continue to focus on this issue.

25. Is the transfer of personal data or PII outside the 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? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

No, the U.S. does not have any data transfer or data localisation requirements. If data is processed outside the U.S., however, that fact should be disclosed in the business' privacy policy.

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The nature and scope of security obligations in the U.S. is still in development, but many laws mandate "reasonable and appropriate security measures." At the federal level, this requirement is found in some sector-specific statutes and regulations. In addition, the FTC has taken the position that it applies broadly to all companies under its jurisdiction by means of the FTC Act, although this is disputed. FTC guidance 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. In a series of FTC enforcement actions, the FTC has asserted that these security programs have 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, access key and secret key management, and secure cloud storage;
- application software design;
- information systems, such as network and software design, information processing, storage, transmission, and disposal;
- review and assessment of as well as response to third-party security vulnerability reports; and
- prevention and detection of as well as response to attacks, intrusions, or other system failures or vulnerabilities.

Following the identification of security risks, FTC guidance indicates that it believes entities must also:

- design and implement "reasonable safeguards" to control 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;
- have 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;
- 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 24 states have laws that address data security practices of private sector entities. Most of these state laws relate to entities that maintain personal information about residents of that state and require the entity to maintain "reasonable security procedures and practices" appropriate to the type of information and the 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. Once fully operative on January 1, 2023, the CPRA will impose on businesses: (i) an affirmative duty to "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure," (ii) a requirement to perform an annual cybersecurity audit and submit a risk assessment to the California Privacy Protection Agency on a regular basis, and (iii) an obligation to contractually obligate third parties with whom the business sells, shares or discloses personal information to provide the same level of privacy protection as required by the CPRA. Similarly in Virginia, Colorado and Utah, once effective, the VCDPA, CPA and UCPA will require controllers to establish, implement, and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data, which are appropriate to the volume and nature of the personal data at issue.

27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

All states in the U.S., 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 unauthorised 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 unauthorised acquisition of personal information. A small number of jurisdictions, including Connecticut, Florida, New Jersey, New York, Puerto Rico and Rhode Island, define security breach as the unauthorised access to personal information. The remaining jurisdictions define it as both unauthorised access to and acquisition of personal information. No state requires notification to individuals or regulators if an incident has not resulted in unauthorised acquisition of or access to personal information.

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 unauthorised 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 unauthorised acquisition of personal information for a lawful purpose is not a security breach unless the personal information is used in an unauthorised manner or subject to further unauthorised disclosure.

For a small number of states, the definition of security breach includes both computerised/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...."

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

In the U.S., "reasonable" security measures are required by many state and federal laws that are specific to particular sectors or types of personal information. At the federal level, for example, HIPAA imposes privacy and security obligations on entities that handle PHI, and GLBA imposes security standards designed to protect "nonpublic personal information" maintained by financial

institutions about their customers. Absent an exception, the Cable Act prohibits cable operators from disclosing PII to third parties without the subscriber's consent, and imposes a general data security obligation on covered entities to prevent unauthorized access to PII. 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 (Energy Policy Act) gave the Federal Energy Regulatory Commission (Commission or 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) cyber security reliability standards. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns.

For federal government corporate and critical infrastructure networks and databases, President Obama issued an executive order, '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 then create and maintain a cybersecurity program based on 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 its critical infrastructure controls and information.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

In the U.S., data breach notification requirements can be complex due to the variety of potentially applicable federal and state laws. All states in the U.S., 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 information." 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 U.S. that requires businesses to report security breaches, there are industry-specific requirements that businesses must comply with. 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." The Securities and Exchange Commission (SEC) requires publicly traded companies to provide "timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision." 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 progress within 24 months, with the final rule due 18 months thereafter.

30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

While there is not a specific and directly applicable law that addresses cyber-crime attacks in the U.S., 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, cyber-crime 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. Additionally, CISA recently issued the "SHIELDS UP" guidance to all organizations which provides 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.

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

No, the U.S. 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.

32. Do the 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 the rights, how they are exercised, what exceptions exist and any other relevant details.

There is no single federal law in the U.S. that sets out individual data privacy rights. The CCPA (and once fully operative on January 1, 2023, the CPRA), however, create a number of individual privacy rights for California residents (called "consumers" under the CCPA) under

certain circumstances to exercise control over their personal information. These consumer rights are not absolute and can be limited when a specific set of exceptions apply. Once effective on January 1, 2023, the VCDPA will provide individual privacy rights to Virginia residents.

Additionally, the CPA (once effective on July 1, 2023) and the UCPA (once effective on December 31, 2023) create a number of individual privacy rights available to Colorado and Utah residents respectively, as discussed below.

California

Applicability

Generally, the CCPA applies to a "business," which is defined as a for-profit entity that does business in California that (i) processes the personal information of California residents (referred to in the CCPA as "consumers"), (ii) decides why and how such personal information is processed, and satisfies at least one of the following criteria:

- Has annual gross revenues over $25 million;
- Buys, receives, sells or shares (for commercial purposes) the personal information of 50,000 or more Californian consumers, households or devices; or
- Derives 50 percent or more of its revenues from selling consumers' personal information.

Where an entity does not meet the definition of a "business," but controls or is controlled by a business, and shares common branding with the business, it will also be subject to the CCPA. Additionally, the definition of "business" is not limited to online enterprises and could be applied to exclusively brick-and-mortar establishments that do business in California.

The CCPA grants California consumers certain rights to know more about how businesses collect, process, disclose and sell the consumer's personal information, to request deletion of personal information and to request to opt-out of the sale of personal information.

The business – not the service provider – is primarily responsible for receiving, analyzing and responding to consumer rights requests under the CCPA. When a company is acting as a "service provider" by processing consumers' personal information solely on behalf of a business subject to a contract prohibiting the company from retaining, using or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, the company is not required to fulfill consumer rights requests of those consumers whose information it processes on behalf of the business.

However, the company may be contractually required or informally asked to assist the business in processing a consumer request. In which case, the CCPA permits the company, while acting as a service provider, to process the request on behalf of the business. In addition, the company should not sell any personal information on behalf of a business when a consumer has opted-out of the sale of their personal information with the business.

It's important to note that once it becomes fully operative in 2023, the CPRA will provide unprecedented rights for California consumers by expanding several consumer rights established by the CCPA as well as adding new consumer rights and protections, including: expanding the right to delete personal information, the right to know categories and specific pieces of personal information, the right to opt-out of the sale or sharing of personal information, the right of nonretaliation; and creating the new right to correct inaccurate information, the right to limit the use and disclosure of sensitive personal information, and the right to opt-out of automated decisionmaking technology.

The CPRA will also revise and expand the scope of covered "businesses" under the CCPA, such as increasing the second quantitative "business" threshold to 100,000 or more consumers or households, and clarifying the indirect "business" definition applies only to entities with whom the business shares consumers' personal information (which further helps to exclude separatelyowned entities). Notably, the CPRA extends the definition of a covered "business" to joint ventures or partnerships and businesses that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, the CPRA.

The Right to Know

The right to know under the CCPA consists of two parts: the right to know the specific pieces of personal information and the right to know the categories of personal information. Upon receipt of a verifiable consumer request, businesses that collect personal information may be required to disclose a list of the specific pieces or categories of personal information collected from the consumer, the sources of such information, the business or commercial purpose for collecting or selling the information, and the categories of third parties to whom the business has shared the personal information. Additionally, upon a verifiable consumer request, a business may be required to provide access to personal information collected by the business, in a format that allows the data to be transmitted to another entity (similar to Europe's GDPR's

requirement of 'data portability').

The CPRA will modify the right to know in two important ways: requiring businesses to provide information about the categories of personal information shared with third parties, where "shared" is defined as providing personal information to a third party for cross-contextual behavioral advertising; and removing the 12-month look-back limitation by requiring businesses to provide more than 12 months of information, so long as such disclosure would not be "impossible" or "involve a disproportionate effort" (though this requirement will not apply to any data collected by the business prior to January 1, 2022).

The Right to Deletion

Under the CCPA, upon a verifiable consumer request, businesses may be required to delete personal information about the consumer and instruct its service providers to delete the consumer's personal information from their records, subject to certain exceptions.

Under the CPRA, this right to deletion will further require a business to notify its service providers and contractors, and also notify any third parties to whom the business has sold or shared (for cross-contextual advertising purposes) the consumer's personal information, unless this "proves impossible or involves disproportionate effort." Additionally, each service provider will be required to notify its own downstream service providers to delete the consumer's personal information.

The CPRA will also expand the exceptions for the right to delete.

The Right to Opt-Out and the Right to Opt-In

Under the CCPA, businesses that sell consumer personal information to third parties (for monetary or other valuable consideration) or disclose consumer personal information to a third party for a business purpose must disclose upon a verifiable consumer request the categories of personal information collected about the consumer, the categories of personal information sold and the categories of third parties to whom each category of personal information was sold, and the categories of personal information that the business disclosed about the consumer for a business purpose. Businesses may be required to instruct its service providers to delete the consumer's personal information from their records, and to honor opt-out requests from consumer to prevent future data sales to third parties (which does not include service providers).

Businesses that sell personal information are required to add a clear and conspicuous link on their homepage titled, 'Do Not Sell My Personal Information,' which takes consumers to an optout tool that prevents their personal information from being sold to third parties.

If the business has actual knowledge that the consumer is under the age of 16, this right becomes the Right to Opt-In, meaning the business cannot sell the personal information without affirmative authorization from the child (for children at least 13 and less than 16 years of age) or the child's parent (for children under 13 years of age).

The CPRA will expand the right to opt-out to include both the sale and the "sharing" of personal information. "Sharing" is defined by the CPRA as the disclosure, transfer or making available of a "consumer's personal information by the business to a third party for purposes of cross-context behavioral advertising, whether or not for monetary or other valuable consideration." Accordingly, the link posted on a business' homepage will need to be updated to reflect this addition and shall be titled "Do Not Sell or Share My Personal Information."

The Right to Limit the Use and Disclosure of Sensitive Personal Information

New under the CPRA is the creation of the separate category of "sensitive personal information." California consumers will have the right to direct a business to limit its use of sensitive personal information to that "which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services," or for the performance of specific enumerated business purposes.

As such, the CPRA will require a second link on the website homepage titled "Limit the Use of My Sensitive Personal Information." In some circumstances, a business may provide a single homepage link that combines this link with the Do Not Sell or Share My Personal Information link to allow consumers to make one or both of these selections. The CPRA also contemplates the creation of an "opt-out preference signal" (additional guidance is expected in the forthcoming regulations).

Right to Opt-Out of Automated Decision-Making Technology

The CPRA directs the California Attorney General to issue regulations governing access and optout rights with respect to the business' use of automated decision-making technology and profiling. The CPRA defines profiling to include any automated processing of personal information to evaluate personal aspects related to a natural person, or to analyze or predict aspects concerning the person's performance at work,

economic situation, health, personal preferences, interests, reliability, behavior, location and movements. The text of the CPRA suggests that such regulations may include a requirement for a business to disclose information about the logic involved in the automated decision-making process in response to a consumer request.

The Right to Correct Inaccurate Information

Similar to Europe's GDPR's Right to Rectification, the CPRA introduces a new right for a consumer to request that a business correct inaccurate personal information maintained by the business. The business will further be required to disclose this new right in its privacy notice.

Once a business receives a verified request to correct inaccurate personal information, the business must use "commercially reasonable efforts" to correct the personal information as directed by the consumer and the adopted regulations.

The Right to Non-Discrimination

Lastly, the right against discrimination is provided under the CCPA to ensure that a consumer is not penalized or retaliated against by the business for exercising their consumer rights.

General Requirements

Businesses' privacy notices should provide consumers with a general explanation of their consumer rights under the CCPA and instructions on how to exercise those rights. Businesses must provide any consumer-requested disclosures within 45 days of the consumer's request, with the possibility of another 45-day extension, and only if the company is able to "reasonably verify" the identity of the consumer making the request. For requests to know, the business should disclose and deliver the requested information collected about the consumer over the 12-month period preceding the receipt of the request, free of charge, in a readily usable format that allows the consumer to transmit the information from one entity to another without hindrance. When transmitting the information to the consumer, the business should use reasonable security measures and should never include "sensitive" pieces of personal information in the response (such as Social Security number, driver's license number or financial account number).

As mentioned above, the CPRA will require a business to provide more than 12 months of information to the extent possible and assuming it does not involve a disproportionate effort.

Additional guidance on revised obligations in accordance with the CPRA is expected from the California Attorney General by July 1, 2022.

Exemptions

Certain types of personal information are not subject to these consumer rights because they fall under an exemption to the CCPA. For example, the following types of personal information could be out of scope for consumer rights requests:

- Personnel Exemption: any personal information collected by a business from a job applicant, employee, controlling owner, director, officer, or contractor in the context of the individual acting as an applicant, employee, controlling owner, director, officer, or contractor of the business. This also includes emergency contact information associated with such a person, as well as information necessary for the business to administer benefits, such as information about the employee's dependents and beneficiaries. Businesses subject to the CCPA law must still provide such persons with notice at or before the point of collection of their information "as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." The business must not collect additional categories of information or use the information for additional purposes not specified in the notice without providing such persons with notice of those new categories and uses. The CPRA extended the date upon which this CCPA exemption was set to expire from January 1, 2021 to January 1, 2023. The California Legislature now has two years to decide whether the personnel exemption will become subject to the CCPA/CPRA in their entirety, or whether an additional temporary or permanent exemption for personnel information is appropriate.
- Business-to-Business ("B2B") Exemption: any personal information that reflects a communication or transaction between a business and the employees of a third-party entity (as well as the controlling owners, directors, officers, and contractors of the third party) occurring within the context of the business providing or receiving a product or service to or from such third-party entity or in the context of conducting due diligence about providing or receiving a product or service. These third-party entity employees continue

to have the right to request to opt-out of sales and the right to non-discrimination for exercising it. The CPRA extended the date upon which the exemption was set to expire from January 1, 2021 to January 1, 2023. The California Legislature now has two years to decide whether the B2B exemption will become subject to the CCPA/CPRA in their entirety, or whether an additional temporary or permanent exemption for B2B information is appropriate.
- Health and Financial Information Exemption: any information subject to enumerated federal or state regulation, such as financial information subject to the GLBA or the California Financial Information Privacy Act (CFIPA), or health or medical information subject to HIPAA or the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The CPRA will also modify existing exemptions under the CCPA, and provide additional exemptions, such as exempting household data from the Right to Know, the Right to Deletion and the Right to Correction. Additionally, the CCPA will allow narrow exemptions specific to certain types of entities.

California's "Shine the Light" Law

In addition to the rights currently granted under the CCPA, consumers may have rights under California's "Shine the Light" Law (Cal. Civ. Code § 1798.83). California's Shine the Light Law primarily requires companies that share California customers' personal information with third parties for those third parties' own direct marketing purposes to either (i) disclose, upon the customer's request, the names and addresses of third parties who have received personal information for their own direct marketing purposes and the categories of personal information transferred for such purposes in the past year or (ii) provide a mechanism for opting into or opting out of the disclosure of personal information to third parties for their own direct marketing purposes.

Virginia

Once effective on January 1, 2023, the VCDPA will introduce novel consumer rights to Virginia residents including the right to access personal data, the right to portability, the right to correction, the right to opt out, and the right to deletion. The VCDPA will require "controllers" to comply with authenticated requests to exercise these rights. "Controllers" are persons that conduct business in Virginia or produce products or services that are targeted to residents of Virginia and that:

- During a calendar year, control or process personal data of at least 100,000 Virginia residents; or
- Control or process personal data of at least 25,000 Virginia residents and derive more than 50 percent of gross revenue from the sale of personal data.

Right to Access

Consumers will have the right to confirm whether or not a controller is processing the consumer's personal data and to access such personal data.

Right to Portability

Consumers will have the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller 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.

Right to Correction

Consumers will have the right to correct inaccuracies in their personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data.

Right to Opt-Out

Consumers will have the right to opt-out of the processing of personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, and (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Right to Deletion

Consumers will have the right to delete personal data provided by or obtained about the consumer.

Right to Appeal

The VCDPA is unique in that it will provide a statutory right to appeal the denial of a consumer rights request. Controllers must establish a process for consumers to appeal the controllers' refusal to process a consumer request within a reasonable period of time. The appeal process must be conspicuously available and similar to the process for submitting a rights request. In the event that a controller denies a consumer's request, the controller must provide an online mechanism, if available, or other method through which the consumer may contact the Virginia Attorney General to submit a complaint.

General Requirements

Similar to the CCPA, the VCDPA mandates that businesses have 45 days to respond to consumer requests and can extend this period for one additional 45-day period when reasonably necessary. If the controller declines to take action regarding the consumer's request, the controller must inform the consumer without undue delay, but no later than 45 days from receipt of the request, and include the reason for declining the request and instructions on how the consumer may appeal the decision to the Virginia Attorney General.

Exemptions

The VCDPA limits the applicability for certain organizations and types of data. An organization is exempt from complying with the VCDPA if it is: (1) a body, authority, board, bureau, commission, district, or Virginian agency or any Virginian political subdivision, (2) a financial institution subject to the GLBA, (3) a covered entity or business subject to HIPAA and HITECH, (4) a nonprofit institution, or (5) an institution of higher education.

The VCDPA also provides exemptions for certain health information regulated by Virginia and federal laws, including HIPAA, as well as specific information regulated by the GLBA, the Fair Credit Reporting Act, Driver's Privacy Protection Act, FERPA, the Farm Credit Act. Lastly, the VCDPA does not apply to data processed by a controller, processor, or third party (i) in the course of an individual applying to, employed by, or acting as an agent of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role; (ii) as the emergency contact information of a personnel used for emergency contact purposes; or (iii) that is necessary for the controller, processor, or third party to retain to administer benefits for another individual relating to the applicable personnel and used for the purposes of administering those benefits.

Colorado

Once effective on July 1, 2023, the CPA will introduce novel consumer rights to Colorado residents including the right to access personal data, the right to correction of personal data, the right to data portability, the right to deletion, the right to opt out and the right to a universal opt-out mechanism. The CPA will require "controllers" to comply with authenticated requests to exercise these rights. "Controllers" are persons that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to residents of Colorado and meet one of the following thresholds:

- During a calendar year, control or process personal data of at least 100,000 Colorado residents; or
- Derive revenue or receive a discount of the price of goods or services from the sale of personal data and control the personal data of at least 25,000 Colorado residents.

Right to Access

Consumers will have the right to confirm whether or not a controller is processing the consumer's personal data and to access such personal data.

Right to Portability

Consumers will have the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable, and to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity.

Right to Correction

Consumers will have the right to correct inaccuracies in their personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data.

Right to Opt-Out

Consumers will have the right to opt-out of the processing of personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, and (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. The CPA's provision of a right to opt out is nearly identical to the VCDPA's right to opt out except for the CPA requirement of controllers to recognize universal opt-out signals as a method for consumers to exercise their opt-out rights.

Effective July 1, 2024, controllers that process personal data for the purposes of targeted advertising or sale must allow consumers to exercise the right to opt out through a user-selected universal opt-out mechanism. The Colorado Attorney General is directed to adopt rules that clarify the technical specifications for such an opt-out mechanism by July 1, 2023.

Right to Deletion

Consumers will have the right to delete personal data concerning the consumer.

Right to Appeal

The CPA mirrors the VCDPA's unique approach in

adopting a statutory right to appeal. The CPA requires that controllers establish internal processes for consumers to appeal a refusal to act on a request to exercise any of the rights above. The appeal process must be made readily available and as easy to use as the process for submitting a request. In the event that a controller denies a consumer's request, the controller must inform the consumer of their ability to contact the Colorado Attorney General if the consumer has any concerns regarding the result of an appeal.

General Requirements

Similar to the CCPA, the CPA mandates that businesses have 45 days to respond to consumer requests and can extend this period for one additional 45-day period when reasonably necessary. If the controller declines to take action regarding the consumer's request, the controller must inform the consumer without undue delay, but no later than 45 days from receipt of the request, and include the reason for declining the request and inform the consumer of their ability to contact the Colorado Attorney General is the consumer has any concerns regarding the result of an appeal.

Exemptions

The CPA limits the applicability of certain organizations and types of data. An organization is exempt from complying with the CPA if it is an air carrier, a financial institution subject to the GLBA or registered with the National Securities Association. Note that there is no entity-level exemption for HIPAA-regulated entities or nonprofit organizations.

The CPA also provides exemptions for certain business-to-business information, and health information regulated by Colorado and federal laws, including HIPAA, as well as specific information regulated by COPPA, the Fair Credit Reporting Act, Driver's Privacy Protection Act, and FERPA. Additionally, the CPA does not apply to data processed by a controller, processor, or third party (i) maintained for employment record purposes; or (ii) that is necessary for the controller, processor, or third party to retain to administer benefits for another individual relating to the applicable personnel and used for the purposes of administering those benefits.

Utah

Once effective on December 31, 2023, the UCPA will introduce novel consumer rights to Utah residents including the right to access and delete personal information, the right to opt out, and the right to data portability. Covered entities will be required to take action on a consumer request within 45 days once-per-year and free of charge. If the request is repetitive, excessive, unfounded, or if the controller "reasonably believes the primary purpose in submitting the request was something other than exercising a right" the controller may charge a fee.

Right to Access

Consumers will have the right to request whether a controller is processing their personal data and obtain access to the personal data.

Right to Delete

Consumers will have the right to direct the controller to delete the personal data provided by the consumer.

Right to Data Portability

Consumers will have the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller, in a format that to the extent technically feasible, is portable; to the extent practicable, is readily usable; and allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means.

Right to Opt Out

The UCPA will grant Utah consumers the right to opt out of the processing of their personal data for targeted advertising or the sale of personal data. Unlike the VCDPA and CPA, the right to opt out of profiling is absent from the UCPA.

Exemptions

The UCPA offers similar exemptions to the VCDPA and CPA, including both entity- and data-level exemptions. In addition, the UCPA offers a similar indefinite B2B and Personnel exemption as the VCDPA and CPA.

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

As mentioned above, there is no federal law in the U.S. that provides individual data privacy rights similar to Europe's GDPR, such as the right to access and the right to deletion. In California, the CCPA, however, does provide a set of consumer rights for California consumers, which may be enforced through the California Attorney General Office or, potentially, a private right of action. The CPRA will modify the CCPA and the authority assigned to the California Attorney General to promulgate regulations under the CPRA will

be exercised by the new California Privacy Protection Agency by the end of April 2022. Notably, the CPRA does not strip the California Attorney General of the enforcement authority that the CCPA provided it. Thus, a business violating the CCPA as amended may alternatively be subject to an injunction and civil penalty (in the same amount as the administrative fine) in a civil action initiated by the Attorney General.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

Currently, there is no comprehensive federal law that provides a private right of action enabling individuals to sue businesses directly for data privacy violations, however, several federal and state privacy laws do allow private rights of action. For example, Illinois' BIPA allows individuals whose biometric data is illegally collected or handled to sue the business responsible. Some state data security breach notification laws and privacy laws requiring "reasonable" security also have a private right of action for violations in limited instances. The CCPA (and, once fully operative, the CPRA) allow a consumer (including employees and third-party entity employees otherwise subject to the Personnel and B2B exemptions) to sue a company for statutory damages where certain of the consumer's nonencrypted and nonredacted personal information is subject to "an 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 adds 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).

At the federal level, for instance, the TCPA provides a private right of action for certain recipients of illegal telephone calls, text messages, or other applicable communications, the Fair Credit Reporting Act provides a private right of action for certain mishandling of consumer background checks or the printing of excessive payment card information on receipts, and the Video Privacy Protection Act 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.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Of the privacy and cybersecurity laws with a private right of action, some require the individual to demonstrate actual injury in order to recover damages, while some, such as BIPA, the CCPA and CPRA, the TCPA and other statutes, award statutory damages to the individual who is subject to the violation of the statute even in the absence of any showing of injury. In regard to the laws that require a showing of injury, courts are divided as to the nature of the injury that is required, but overall individuals have tended to find more success when they have been able to point to monetary damage than when they have pointed to less tangible forms of injury such as emotional harm, lost time or a loss of privacy.

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 give a plaintiff standing, but is typically insufficient to satisfy the injury element of a claim, if any. Courts are also divided on whether and when the plaintiff's being subject to a violation of a statute is a sufficient injury in and of itself to give an individual standing.

36. How are the laws governing privacy and data protection enforced?

Federal and state privacy laws are generally enforced at the federal and state levels, respectively. At the federal level, enforcement is typically handled by the FTC, although other agencies and/or state attorneys general may also enforce certain laws. For example, HIPAA is enforced by the federal Department of Health & Human Services and state attorneys general. The FTC may pursue companies for violations of particular U.S. privacy and cybersecurity laws and has claimed authority to bring enforcement actions over the privacy and cybersecurity practices of all companies under its jurisdiction via Section 5 of the FTC Act (prohibiting deceptive and unfair practices). When it proceeds under

the FTC Act for a first-time violation, the FTC generally may obtain only an injunction or order to cease and desist, but can also potentially obtain disgorgement or restitution if it meets certain requirements. It cannot impose penalties for firsttime violations of Section 5, but can do so for violation of certain of the sector-specific privacy statutes it enforces. A company who 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 privacy and cybersecurity laws typically falls to the state attorney general, situated within the state's chief law enforcement body, its justice department. There is substantial variation in enforcement power and actions among the different state regulators. Certain states, such as California, Connecticut, Illinois, Massachusetts and New York, are the most active in enforcing privacy laws, as these states also have some of the most robust privacy laws in the U.S. Generally speaking, most enforcement actions and settlements are made public. For example, the State of California Department of Justice has a privacy enforcement actions page. Individual state privacy laws set out the range of fines or penalties that may be issued and may provide for equitable remedies, such as injunction, as well as monetary fines. Fines at the state level are usually issued on a per-violation basis.

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

Below is a summary of the penalties laid out in several key federal privacy 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 $127 per violation, up to $63,973; (2) the violation was due to reasonable cause, a minimum of $1,280 per violation, up to $63,973; (3) the violation was due to willful neglect but corrected within 30 days, a minimum of $12,794 per violation, up to $63,973; and (4) the violation was due to willful neglect and not corrected within 30 days, a minimum of $63,973 per violation, up to $1,919,173. 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 $1,919,173. Data breaches resulting from a violation may trigger additional fines. 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 $46,517 per violation, generally, for each child whose personal information was collected in violation of the statute, in addition to non-monetary 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 provide for lower penalty amounts.

Below is a summary of the penalties laid out in several key state privacy laws:

- CalOPPA: The penalty for non-compliance is a maximum of $2,500 per violation.
- CCPA: The CCPA subjects violators to civil penalties of $2,500 per violation, $7,500 if intentional.
- CPRA: The CPRA will increase the CCPA's fines to $7,500 for "violations involving the personal information of consumers whom the business, service provider, contractor or other person has actual knowledge is under 16 years of age." As a result, ordinary CPRA violations relating to children's personal information will be subject to three times the monetary fines currently available under the CCPA.
- VCDPA: The Virginia Attorney General may initiate an action for violation of the VCDPA, and may seek an injunction to restrain any

violations of the VCDPA and civil penalties of up to $7,500 for each violation of the VCDPA.
- CPA: Enforcement authority under the CPA is delegated to both the Colorado Attorney General and district attorneys. Violations of the CPA are considered a deceptive trade practice under the Colorado Consumer Protection Act which allows for penalties up to $20,000 per violation.
- UCPA: The Utah Attorney General may initiate an enforcement action and impose penalties of actual damages and fines up to $7,500 per violation.

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

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

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

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

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

The court of appeals and, if applicable, the Supreme Court, may in some situations confer deference to the findings or conclusions of the regulator.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

Other states are considering CCPA-inspired legislation this year, including Connecticut. In addition, the California state legislature proposed two bills to extend the existing CCPA and CPRA employee and B2B data exemptions to January 1, 2026, or indefinitely. The California state legislature adjourns on August 31, 2022, so it will have until that time to consider the passage of either bill.

Contributors

Heather Sussman
Partner
hsussman@orrick.com

Sulina Gabale
Partner
sgabale@orrick.com

Thora Johnson
Partner
thora.johnson@orrick.com

Tori Downey
Associate
tori.downey@orrick.com

Kathryn Boyle
Associate
kboyle@orrick.com

Oladoyin Olanrewaju
Associate
oolanrewaju@orrick.com