The Legal 500 Country Comparative Guides

United States: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection & cyber security laws and regulations that may occur in United States.

For a full list of jurisdictional Q&As visit here

Contributing Firm

Orrick, Herrington & Sutcliffe LLP

Authors

Heather Egan Sussman
Partner

hsussman@orrick.com

David T. Cohen
Of Counsel

david.cohen@orrick.com

Tori Downey
Associate

tori.downey@orrick.com

1. **Please provide an overview of the legal and regulatory framework governing 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)?**

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 pre-emption 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, 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.

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 Department of Health & Human Services 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. 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's practices regarding their own personal information upon verified request. In addition, companies may not discriminate against California consumers who exercise their CCPA rights. Other states are considering CCPA-inspired legislation, and federal consumer privacy legislation is also under consideration.

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, 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 self-regulatory principles enforced by the Digital Advertising Alliance (DAA) and the Network Advertising Initiative (NAI). The DAA has developed and enforces privacy practices for digital advertising, providing consumers with enhanced transparency. To use the DAA's advertising option icon, however, requires a license. The NAI has established and enforces self-regulatory standards among its members.

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 personal 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 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 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, 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, demographics and classifications, usage data, 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. 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?**

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's 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 FTC Act authority to enforce promises made by businesses in their privacy notices.

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

5. **Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there are rules relating to the form, content and administration of such consent?**

   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-to-business).

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 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.

7. **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 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 and connected toys) 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; and 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. COPPA also places limits on the use of personal information collected online from children for direct marketing purposes.

In addition, FERPA governs how schools collect, use and disclose information from students' educational records, including information collected about children or minors. FERPA sets forth certain rights and restrictions concerning the disclosure of students' educational information – which generally requires written consent – and how parents and students may access, revise 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 submitted online. Michigan and Utah have Child Protection Registry Acts. And several states have laws governing schools' and third-party contractors' collection, use, disclosure and sale of educational information. In addition, under the CCPA, businesses may not sell PI of California residents under the age of 16 without their or, in the case of children under 13, their parent's opt-in consent.

8. **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 new CCPA has exclusions of various degrees for data governed by HIPAA, GLBA, FCRA, and other state and federal laws.

9. **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. does not impose requirements of data protection by design or default. 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.

10. **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).

11. **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.

12. **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 explicitly required only for certain industries in a limited number of jurisdictions. However, security risk assessments can help an organization achieve, and sometimes are necessary to achieve, the reasonable security required by a myriad of state and federal laws. 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). 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.

13. **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.

14. **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, business-to-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. More than a dozen other states are considering similar laws, as is Congress.

15. **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?)**

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, FERPA 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. Finally, 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.

16. **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)?**

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.

17. **Please describe any restrictions on monitoring 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 or profiling generally have not historically restricted these activities, but rather regulate or require disclosures regarding the use of cookies and other tracking technologies. The CCPA is positioned to change this by providing an opt-out of the selling of data, which as currently defined and interpreted would be implicated by many interest-based advertising activities.

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. Recently, 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.

In addition, ECPA, SCA and CFAA, 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, although that law is evolving.

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.

18. **Please describe any laws in your jurisdiction addressing 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 Telemarking 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 nonmarketing 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 pre-empts 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.

19. **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.

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.

20. **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 cross-border transfer of personal data or PII require notification to or authorization form 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.

21. **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.

22. **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) what types of personal information are protected under 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.

A majority of the jurisdictions with breach notification laws define security breach as involving the unauthorised acquisition of personal information. A small number of jurisdictions, including Connecticut, Florida, New Jersey, 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.…"

23. **Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?**

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. 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.

24. **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." Lastly, the NYDFS Cybersecurity Regulation requires registered financial institutions to report a security breach within 72 hours of becoming aware of the breach.

25. **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 (ie, the violator knowingly and intentionally spread the ransomware).

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.

26. **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.

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, however, creates 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.

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.

27. 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.

The Right to Know

The right to know 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 General Data Protection Regulation's (GDPR) requirement of 'data portability').

The Right to Deletion

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.

The Right to Opt-Out and the Right to Opt-In to Personal Information Sales

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 opt-out 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 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).

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. This limited carve out is currently set to expire as of January 1, 2021 when such information will become subject to the full scope of the law.

- **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. This limited carve out is currently set to expire as of January 1, 2021 when such information will become subject to the full scope of the law.

- **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.

California's "Shine the Light" Law

In addition to the rights 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.

28. **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. California's CCPA, however, does provide a set of consumer rights for California consumers, which are enforced through the California Attorney General Office or a private right of action.

29. **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. The CCPA allows a consumer (including employees and third-party entity employees otherwise subject to the Personnel and B2B exemptions) to sue a company for statutory damages in certain situations where 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". Some state data security breach notification laws and laws requiring "reasonable" security also have a private right of action.

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.

30. **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, 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.

31. **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 first-time 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.

32. **What is the range of 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 factors, including the flagrancy of the violation and any mitigating steps the entity may have taken. Fines are issued in four categories: (1) minimum of $100 per violation, up to $50,000; (2) minimum of $1,000 per violation, up to $50,000; (3) minimum of $10,000 per violation, up to $50,000; and (4) minimum of $50,000 per violation. Fines are generally issued on a per-violation

basis, per year that the violation occurred. The maximum fine per category, per year is $1,500,000. 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 category per year. HIPAA violations may also carry criminal penalties.
    - COPPA: Courts may hold operators liable for civil penalties up to $42,530 per violation. Penalties are 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.

The CCPA subjects violators to civil penalties of $2,500 per violation, $7,500 if intentional. (It is still unclear what a "violation" is under the CCPA.)

33. **Can personal data or PII owners/controller 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.