Data Protection Laws and Regulations USA 2024

ICLG - Data Protection Laws and Regulations - USA Chapter covers common issues including relevant legislation and competent authorities, territorial scope, key principles, individual rights, registration formalities, appointment of a data protection officer and processors.

Published: 31/07/2024

Chapter Content Free Access

1. Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There is no single principal data protection legislation in the United States (U.S.). Rather, a jumble of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of U.S. residents. At the federal level, the Federal Trade Commission Act (FTC Act) (15 U.S. Code § 41 *et seq.*) broadly empowers the U.S. Federal Trade Commission (FTC) to bring enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations. The FTC has taken the position that "deceptive practices" include a company's failure to comply with its published privacy promises and its failure to provide adequate security of personal information, in addition to its use of deceptive advertising or marketing methods.

As described more fully below, other federal statutes primarily address specific sectors, such as financial services or healthcare. In parallel to the federal regime, state-level statutes protect a wide range of privacy rights of individual residents. The protections afforded by state statutes often differ considerably from one state to another, and some are comprehensive, while others cover areas as diverse as protecting library records to keeping homeowners free from drone surveillance.

1.2 Is there any other general legislation that impacts data protection?

Although there is no general federal legislation impacting data protection, there are a number of federal data protection laws that are sector-specific (see question 1.3 below), or focus on particular types of data. By way of example, the Driver's Privacy Protection Act of 1994 (18 U.S. Code § 2721 *et seq.*) governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles. Children's information is protected at the federal level under the Children's Online Privacy Protection Act (COPPA) (15 U.S. Code § 6501), which prohibits the collection of any information from a child under the age of 13 online and from digitally connected devices, and requires publication of privacy notices and collection of verifiable parental consent when information from children is being collected. The Video Privacy Protection Act (18 U.S. Code § 2710 *et seq.*) restricts the disclosure of rental or sale records of videos or similar audio-visual materials, including online streaming. Similarly, the Cable Communications Policy Act of 1984 includes provisions dedicated to the protection of subscriber privacy (47 U.S. Code § 551). Finally, even in the absence of legislation, presidential administrations are often active with rulemaking, executive orders and other authorities. For example, in the past two years, the Biden-Harris administration has released its National Cybersecurity Strategy and also issued an Executive Order laying out principles for privacy and security in developing and deploying artificial intelligence.

State laws also may impose restrictions and obligations on businesses relating to the collection, use, disclosure, security or retention of special categories of information, such as biometric data, medical records, social security numbers, driver's licence information, email addresses, library records, television viewing habits, financial records, tax records, insurance information, criminal justice information, phone records and education records, to name some of the most common.

Every state has adopted data breach notification legislation that applies to certain types of personal information about its residents. Even if a business does not have a physical presence in a particular state, it typically must comply with the state's laws when faced with the unauthorised access to, or acquisition of, personal information it collects, holds, transfers or processes about that state's residents. The types of information subject to these laws vary, with most states defining personal information in the data breach context to include an individual's first name or first initial and last name, together with a data point including the individual's SSN, driver's licence or state identification card number, financial account number or payment card information.

Some states are more active than others when it comes to data protection. Massachusetts, for example, has strong data protection regulations (201 CMR 17.00), requiring any entity that receives, stores, maintains, processes or otherwise has access to "personal information" of a Massachusetts resident in connection with the provision of goods or services, or in connection with employment, (a) to implement and maintain a comprehensive written information security plan addressing 10 core standards, and (b) to establish and maintain a formal information security programme that satisfies eight core requirements, which range from encryption to information security training.

In 2019, New York expanded its data breach notification law to include the express requirement that entities develop, implement and maintain "reasonable" safeguards to protect the security, confidentiality and integrity of private information. Significantly, New York's Stop Hacks and Improve Electronic Data Security Act (N.Y. Gen Bus. Law § 899-bb) identified certain administrative, technical and physical safeguards which, if implemented, are deemed to satisfy New York's reasonableness standard under the law. Previously, New York prioritised the regulation of certain financial institutions doing business in the state, by setting minimum cybersecurity standards, with requirements for companies to perform periodic risk assessments and file annual compliance certifications (23 NYCRR 500). In 2023, the New York Department of Financial Services

(NYDFS) adopted final amendments to its revised Cybersecurity Requirements for Financial Services Companies, which includes banks, financial services and insurance companies, among other entities.

Illinois has a uniquely expansive state law (740 ILCS 14), which imposes requirements on businesses that collect or otherwise obtain biometric information and allows private individuals to sue and recover damages for violations. In January 2019, the Illinois Supreme Court offered an expansive reading of the protections of the Illinois Biometric Privacy Act (BIPA), holding that the law does not require individuals to show they suffered harm other than a violation of their legal rights to sue. Recent decisions have continued the trend toward an expansive reading of BIPA. In February 2023, the Illinois Supreme Court held that a company violated BIPA every time it took employees' fingerprints to clock in and out of their shifts, not simply once for each affected employee. Also in February 2023, the Illinois Supreme Court held that claims brought under BIPA are subject to a five-year statute of limitations.

Washington recently passed a comprehensive health information-related law with broad scope and application. The Washington My Health My Data Law (WMHMYDA) aims to safeguard consumer health data beyond the scope of the federal Health Insurance Portability and Accountability Act (HIPAA) by regulating the collection, sharing and selling of consumer health data by any entity that conducts business or controls or processes consumer health data, in Washington. The WMHMYDA notably provides for a private right of action for consumers to seek actual (not statutory) damages, while authorising courts to impose treble damages up to a maximum of US$25,000.

California has a long history of adopting privacy-forward legislation, and in 2018, the state enacted the California Consumer Privacy Act (CCPA), which became effective on January 1, 2020. The law introduced new obligations on covered businesses, including requirements to disclose the categories of personal information the business collects about consumers, the specific pieces of personal information the business collected about

the consumer, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting or selling personal information, and the categories of third parties with which the business shares personal information. It also introduced new rights for California residents, including the right to request access to and deletion of personal information and the right to opt out of having personal information sold to third parties.

More recently, we have seen a number of states push towards enacting similar comprehensive consumer data privacy laws. Specifically, in 2020, California amended the CCPA with the California Privacy Rights Act (CPRA), which expanded the rights granted to consumers and increased compliance obligations on businesses. In 2021, Virginia enacted the Consumer Data Protection Act (Virginia CDPA), becoming the second state with a comprehensive data privacy law, followed shortly thereafter by Colorado, which enacted the Colorado Privacy Act. Continuing this trend, in 2022, Utah enacted the Utah Consumer Privacy Act and Connecticut enacted an Act Concerning Personal Data Privacy and Online Monitoring (Connecticut Privacy Act). In 2023, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, and Texas all passed state comprehensive consumer data privacy laws. In 2024, Kentucky, New Hampshire and New Jersey have passed such laws. In the absence of a data privacy framework at the federal level, states continue to pursue legislation. In addition, state regulators are also actively making rules to implement these laws, with final rulemaking from California and Colorado, for example, becoming effective in 2023. As of July 1, 2024, the laws from California, Colorado, Connecticut, Florida, Oregon, Texas, Utah and Virginia will all be effective, with Montana due to become effective on October 1, 2024.

1.3 Is there any sector-specific legislation that impacts data protection?

Key sector-specific laws include those covering financial services, healthcare, telecommunications and education.

The Gramm Leach Bliley Act (GLBA) (15 U.S. Code § 6802(a) *et seq.*) governs the protection of personal information in the hands of banks, insurance companies and other companies in the financial service industry. This statute addresses "Non-Public Personal Information" (NPI), which includes any information that a financial service company collects from its customers in connection with the provision of its services. It imposes requirements on financial service industry companies for securing NPI, restricting disclosure and use of NPI and notifying customers when NPI is improperly exposed to unauthorised persons.

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (15 U.S. Code § 1681), restricts use of information with a bearing on an individual's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to determine eligibility for credit, employment or insurance. It also requires the truncation of credit card numbers on printed receipts, requires the secure destruction of certain types of personal information, and regulates the use of certain types of information received from affiliated companies for marketing purposes.

In addition to financial industry laws and regulation, the major credit card companies require businesses that process, store or transmit payment card data to comply with the Payment Card Industry Data Security Standard.

The HIPAA, as amended (29 U.S. Code § 1181 *et seq.*) protects information held by a covered entity that concerns health status, provision of healthcare or payment for healthcare that can be linked to an individual. Its Privacy Rule regulates the collection and disclosure of such information. Its Security Rule imposes requirements for securing this data.

The Telephone Consumer Protection Act (TCPA) (47 U.S. Code § 227) and associated regulations regulate calls and text messages to mobile phones, and regulate calls to residential phones that are made for marketing purposes or using automated dialling systems or pre-recorded messages. Relatedly, the Controlling the Assault of Non-Solicited Pornography and

Marketing Act (CAN-SPAM Act) (15 U.S. Code § 7701 *et seq.*) and associated regulations set basic rules for sending commercial emails, including providing an opt-out right to recipients.

The Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) provides students with the right to inspect and revise their student records for accuracy, while also prohibiting the disclosure of these records or other personal information on the student, without the student's or parent's (in some instances) consent.

Where a federal statute covers a specific topic, the federal law may pre-empt any similar state law on that topic. However, certain federal laws, like the GLBA for instance, specify that they are not pre-emptive of state laws on the subject.

1.4 What authority(ies) are responsible for data protection?

While the U.S. has no plenary data protection regulator, the FTC's authority is very broad, and often sets the tone on federal privacy and data security issues. In addition, a variety of other agencies regulate data protection through sectoral laws, including the Office of the Comptroller of the Currency, the Department of Health and Human Services (HHS), the Federal Communications Commission (FCC), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (CFPB) and the Department of Commerce. At the state level, the CPRA established the first dedicated privacy regulator in the U.S., the California Privacy Protection Agency (CPPA). The CPPA's responsibilities include enforcement of the CPRA with the California Attorney General, rulemaking under the CPRA, and promoting public awareness of privacy issues. Other states have continued to authorise their Attorneys General to conduct rulemaking or to bring enforcement actions related to violations of their respective data privacy law.

2. Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**": In the U.S., information relating to an individual is typically referred to as "personal information" (rather than personal data), though notably, recent privacy legislation from states including Virginia, Colorado, Utah and Connecticut use the term "personal data". The definition of personal information in the U.S. is not uniform across all states or all regulations. In addition, certain data may be considered personal information for one purpose but not for another.
- "**Processing**": The definition of processing in the U.S. is not uniform across all states or all regulations. The general concept encompasses any operations performed on personal information or data, including collection, use, storage, disclosure, transfer, analysis, etc.
- "**Controller**": Unlike California, more recent states, including in Virginia, Colorado, Utah and Connecticut, have incorporated this term in their data privacy legislation. Though definitions may vary, the general concept refers to the entity that determines the purpose and means of processing personal information.
- "**Processor**": Unlike California, more recent states, including in Virginia, Colorado, Utah and Connecticut, have incorporated this term in their data privacy legislation. Though definitions may vary, the general concept refers to an entity that processes personal information on behalf of a controller.
- "**Data Subject**": The state data protection statutes typically cover a "consumer" residing within the state. The definition of "consumer" differs by state. Under most state data protection statutes, a "consumer" is an individual resident of the state and who engages with a business for personal, family or household purposes. In contrast, under the CCPA, a "consumer" is defined broadly as a "natural person who is a California resident".

- "**Sensitive Personal Data**"/"**Special Categories of Personal Data**": The definition of processing in the U.S. is not uniform across all states or all regulations. For those jurisdictions that consider sensitive personal data, it refers to personal information of heightened concerns, potentially including racial or ethnic origin, genetic or biometric data, citizenship, sexual orientation, health information, information in children, online browsing data or precise geolocation data.
- "**Data Breach**": The definition of a data breach depends on the individual state statute, but typically involves the unauthorised access or acquisition of computerised data that compromises the security, confidentiality or integrity of personal information.

3. Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Businesses established in other jurisdictions may be subject to both federal and state data protection laws for activities impacting U.S. residents whose information the business collects, holds, transmits, processes or shares.

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

State comprehensive data privacy laws generally set thresholds (such as gross revenue from the sale of personal data or the number of consumers whose data is controlled or processed) under which all processing activities are carved out from the laws' requirements. Additionally, many exempt processing from several categories of entities covered by other laws, including state and city government agencies, certain financial institutions, non-profit organisations and institutions of higher education,

though these entities' processing activities may be governed by other sector-specific federal or state data protection laws.

4. Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**: The FTC has issued guidelines espousing the principle of transparency, recommending that businesses: (i) provide clearer, shorter and more standardised privacy notices that enable consumers to better comprehend privacy practices; (ii) provide reasonable access to the consumer data they maintain that is proportionate to the sensitivity of the data and the nature of its use; and (iii) expand efforts to educate consumers about commercial data privacy practices.
- **Lawful basis for processing**: While there is no "lawful basis for processing" requirement under U.S. law, the FTC recommends that businesses provide notice to consumers of their data collection, use and sharing practices and obtain consent in limited circumstances where the use of consumer data is materially different than claimed when the data was collected, or where sensitive data is collected for certain purposes. Certain new state laws require obtaining consent in certain circumstances, such as prior to processing sensitive personal data.
- **Purpose limitation**: The FTC recommends privacy-by-design practices that include limiting "data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law".
- **Data minimisation**: See above. In addition, the CPPA issued guidance noting that data minimisation is a foundational principle in the CCPA that applies to each purpose for which a business collects, uses, retains and shares personal information, and the processing of consumer's CCPA requests.

- **Proportionality**: See above.
- **Retention**: The FTC recommends privacy-by-design practices that implement "reasonable restrictions on the retention of data", including disposal "once the data has outlived the legitimate purpose for which it was collected". Additionally, state laws may also specify specific retention parameters, for example, Texas's Capture or Use of Biometric Identifier Act requires the destruction of biometric identifiers within a reasonable time, but not more than a year after the purpose for capturing the biometric identifiers has ended.
- **Accuracy**: The FTC has enforced the FTC Act against data brokers making false claims about the accuracy of their data, such as on a credit report and businesses that inaccurately describe their collection and processing of personal data. State comprehensive data privacy laws offer consumers the right to correct inaccuracies in their personal data.
- **Other key principles**: This is not applicable in our jurisdiction.

5. Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**: These rights are statute-specific. For example, under certain circumstances, employees are entitled to receive copies of data held by employers. In other circumstances, parents are entitled to receive copies of information collected online from their children under the age of 13. Under the HIPAA, individuals are entitled to request copies of medical information held by a health services provider. At the state level, the CCPA provides a right of access to California residents for personal information held by a business relating to that resident. Other state privacy laws, including the Virginia CDPA, Colorado Privacy Act, Utah

Consumer Privacy Act and the Connecticut Privacy Act, provide a similar right.

- **Right to rectification of errors**: These rights are statute-specific. Some laws, such as the FCRA, provide consumers with a right to review data about the consumer held by an entity and request corrections to errors in that data. At the state level, the right to correct information commonly attaches to credit reports, as well as criminal justice information, employment records and medical records. State data privacy legislation, including the CCPA, Virginia CDPA, Colorado Privacy Act and the Connecticut Privacy Act, provide a consumer the right to correct inaccuracies in personal data held by a business.
- **Right to deletion/right to be forgotten**: These rights are statute-specific. By way of a federal law example, the COPPA provides parents the right to review and delete their children's information and may require that data be deleted even in the absence of a request. Some state laws, such as the CCPA, provide a right of deletion for residents of the respective states, with certain exceptions. Recent state privacy laws, including the CPRA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act, provide a similar right to delete.
- **Right to object to processing**: These rights are statute-specific. Individuals are given the right to opt out of receiving commercial (advertising) emails under the CAN-SPAM Act and the right to not receive certain types of calls to residential or mobile telephone numbers without express consent under the TCPA. Some states provide individuals with the right not to have telephone calls recorded without either consent of all parties to the call or consent of one party to the call. Under the CCPA, consumers have the right to opt out of the sale of personal information and the processing of sensitive information (in certain circumstances).
- **Right to restrict processing**: These rights are statute-specific. Certain laws restrict how an entity may process consumer data. For example, the CCPA allows California residents, and the Nevada Privacy Law allows Nevada residents, to prohibit a business from

selling that individual's personal information. Recent state privacy laws, including the Virginia CDPA, Colorado Privacy Act and Connecticut Privacy Act, provide a right to restrict processing for the purposes of sale, targeted advertising and profiling. The CCPA allows consumers to opt out of the processing of sensitive personal information except for certain specific purposes. The Utah Consumer Privacy Act provides a slightly narrower right to restrict processing for the purposes of sale or targeted advertising.

- **Right to data portability**: These rights are statute-specific. Examples of consumer rights to data portability exist under the HIPAA, where individuals are entitled to request that medical information held by a health services provider be transferred to another health services provider. In addition, state privacy laws, including the CCPA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act, provide a right to data portability.
- **Right to withdraw consent**: These rights are statute-specific. By way of example, under the TCPA, individuals are permitted to withdraw consent required to permit a business to send certain types of calls or texts to residential or mobile telephone lines. For an example under state law, the Colorado Privacy Act requires that consumers have the right to withdraw consent, because the regulations do not consider consent that a consumer cannot easily withdraw, to "be freely given". Other state laws, such as the CCPA, address the right to withdraw consent by empowering users to limit the processing of sensitive personal data at any time.
- **Right to object to marketing**: These rights are statute-specific. Several laws permit consumers to restrict marketing activities involving their personal data. Under the CAN-SPAM Act, for example, individuals may opt out of receiving commercial (advertising) emails. Under the TCPA, individuals must provide express written consent to receive marketing calls/texts to mobile telephone lines. California's Shine the Light Act requires companies that share personal information for the recipient's direct marketing purposes to either provide an opt-out or make certain

disclosures to the consumer of what information is shared, and with whom. State privacy laws, including the CCPA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act, provide consumers with the right to opt out of processing of their personal information for targeted advertising.

- **Right protecting against solely automated decision-making and profiling**: State privacy rules against profiling, including in California, Virginia, Colorado and Connecticut, became effective for the first time in 2023.
- **Right to complain to the relevant data protection authority(ies):** These rights are statute-specific. By way of example, individuals may report unwanted or deceptive commercial email ("spam") directly to the FTC, and telemarketing violations directly to the FCC. Similarly, anyone may file a HIPAA complaint directly with the HHS. At the state level, California residents may report alleged violations of the CCPA to the California Attorney General or the CPPA. Similarly, the Utah Consumer Privacy Act provides that Utah residents may report alleged violations to the state's Consumer Protection Division.
- **Other key rights**: This is not applicable in our jurisdiction.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

This is not applicable in our jurisdiction. A few U.S. data privacy laws allow for individuals to institute an action for violations of data privacy statutes or regulations, including actions that could take the form of a class action or collective redress. However, most U.S. data privacy laws do not authorise such individual actions. Rather, the trend under U.S. data privacy laws is to restrict enforcement to regulators.

6. Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Children's information is protected at the federal level under the COPPA (15 U.S. Code § 6501). The COPPA requires operators of: (a) commercial websites and online services directed to children under the age of 13; or (b) general or mixed audience commercial websites or online services with actual knowledge they are collecting personal information from children under the age of 13 to meet specific compliance obligations where they collect personal information from children under the age of 13. Specifically, the COPPA requires that covered operators: (1) publish certain privacy notices, including a COPPA-compliant privacy policy and "direct notice" to parents prior to the collection of personal information from their child; (2) obtain parental consent prior to collecting personal information from a child under the age of 13; (3) provide parents a choice regarding disclosure of a child's information to third parties under certain circumstances; (4) provide parents access to their child's personal information and opportunities to delete that information or prevent further use or collection of a child's information; and (5) maintain the confidentiality, security and integrity of the information collected.

At the state level, the CCPA alters its right to opt out of sale of personal information for consumers under the age of 16. Businesses are prohibited from selling personal information of consumers under the age of 16 without affirmative authorisation from a consumer aged 13–15 or from the parent or legal guardian of a consumer under the age of 13. Recent privacy laws, including in Virginia, Colorado, Utah and Connecticut, consider the personal data of a child below the age of 13 as sensitive personal data. In Virginia, Utah and Connecticut, controllers must process a child's data in accordance with the COPPA. The Colorado Privacy Act requires consumer consent before processing sensitive personal data, but notably exempts personal data subject to the COPPA. In 2022, California enacted the Age-Appropriate Design Code Act, which imposes requirements addressing transparency requirements, default settings and data protection impact assessments. Notably, the law, effective July 1,

2024, applies to children under 18, not under 13 like the COPPA or other laws involving children's data.

7. Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Both Vermont and California require data brokers to register with the respective Attorneys General. The Vermont requirement defines a "data broker" to include entities that knowingly collect and sell or license to third parties the personal information of a consumer with whom the business does not have a direct relationship (9 V.S.A. chapter 62). California's data broker definition similarly encompasses the knowing collection and sale of personal information regarding consumers with which the business does not have a direct relationship (Cal. Civ. Code § 1798.99.80(d)).

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The states that have mandated data broker registration generally do not require a specific description of relevant data processing activities. California makes it optional for the data broker to provide within its registration any information concerning its data collection practices (Cal. Civ. Code § 1798.99.82). Vermont, in contrast, is more demanding and requires registrants to disclose information regarding consumer opt-out, whether the data broker implements a purchaser credentialling process, and the number and extent of any data broker security breaches it experienced during the prior year. Where data brokers knowingly possess information about minors, Vermont law requires that they detail all related data collection practices, databases, sales activities and opt-out policies (9 V.S.A. § 2446).

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Data broker registrations are made on a "per legal entity" basis.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Within the states for which it applies, registrations are required based on the business falling within the definition of a "data broker" pursuant to state law. Generally, a "data broker" is defined as a business that knowingly collects and sells the personal information of a consumer with whom the business does not have a direct relationship.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

See question 7.2 above.

7.6 What are the sanctions for failure to register/notify where required?

In Vermont, the penalty is US$50 per day in addition to the registration fee of US$100. In California, a data broker that fails to register is liable for civil penalties, fees and costs of US$100 for each day the data broker fails to register and an amount equal to the fees that were due during the period it failed to register.

7.7 What is the fee per registration/notification (if applicable)?

Fees vary by state. The data broker registration fee in Vermont is US$100 and in California it is US$400.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

In both Vermont and California, data brokers are required to register annually.

7.9 Is any prior approval required from the data protection regulator?

Data broker registration submissions require Attorney General approval in both Vermont and California.

7.10 Can the registration/notification be completed online?

Data broker registration for both Vermont and California may be completed online.

7.11 Is there a publicly available list of completed registrations/notifications?

Vermont and California maintain publicly available lists of registered data brokers.

7.12 How long does a typical registration/notification process take?

Neither Vermont nor California publish information concerning the typical amount of time for the data broker registration process.

8. Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Appointment of a Data Protection Officer is not required under U.S. law, but certain statutes require the appointment or designation of an individual or individuals who are charged with compliance with the privacy and data security requirements under the statute. These include the GLBA, HIPAA and the Massachusetts Data Security Regulation, for example.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Potential sanctions are statute/regulator-specific.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable in our jurisdiction.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable in our jurisdiction.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in our jurisdiction.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable in our jurisdiction.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable in our jurisdiction.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

This is not applicable in our jurisdiction.

9. Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Under certain state laws and federal regulatory guidance, if a business shares certain categories of personal information with a vendor, the business is required to contractually bind the vendor to reasonable security practices. The HIPAA, for example, requires the use of Business Associate Agreements for the transfer of protected health information to vendors. State laws such as the CCPA, Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act require written contracts for certain entities that process personal information for the business/controller.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The form of the contract typically is not specified. The HIPAA, however, is an example of a federal statute with minimum requirements for provisions that must be included within Business Associate Agreements. These agreements must include limitations on use and disclosure, and require vendors to abide by the HIPAA's Security Rule, to provide breach notification and report on unauthorised use and disclosure, to return or destroy protected data, and to make its books, records and practices available to the federal regulator. Requirements under state data privacy legislation vary by jurisdiction. Under the CCPA, the contract must restrict the service provider from retaining, using or disclosing personal information for any purpose other than performance of the services specified in the contract. Additional mandatory contract provisions on both service providers and contractors include requiring that contracts prohibit service providers from selling or sharing personal information and from retaining, using or disclosing personal information outside of the direct business relationship between the business and the service provider, allowing review or audits of service provider or contractors' data processing practices to ensure compliance and assisting businesses with complying with consumer rights requests. Additionally, state laws such as the Virginia CDPA, Colorado Privacy Act, Utah Consumer Privacy Act and the Connecticut Privacy Act each require that a contract set forth instructions for processing, including the type of data subject to processing and the nature and purpose of processing, and set specific requirements regarding engagement of subcontractors. The Colorado Privacy Act further requires that controllers and processors implement appropriate technical and organisational safeguards related to security.

10. Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Prior express written consent is required under the TCPA before certain marketing texts may be sent to a mobile telephone line. Other federal statutes have opt-out rather than opt-in consent requirements. For instance, under the CAN-SPAM Act, marketing emails – or emails sent for the primary purpose of advertising or promoting a commercial product or service – may be sent to those not opting out, provided the sender is accurately identified, the subject line and text of the email are not deceptive, the email contains the name and address of the sender, the email contains a free, simple mechanism to opt out of future emails, and the sender honours opt-outs within 10 days of receipt.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The TCPA and CAN-SPAM Act apply to both business-to-consumer and business-to-business electronic direct marketing. In contrast, business-to-business telephone communications, except those intended to induce the retail sale of non-durable office or cleaning supplies, are exempt from the Telemarketing Sales Rule described in question 10.3 below.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Marketing by telephone is regulated on the national level by the Telemarketing Sales Rule, a regulation under the Telemarketing and Consumer Fraud and Abuse Prevention Act. This act established the national Do Not Call (DNC) list of telephone numbers that cannot be used for marketing communications (calls and texts) and disclosure requirements for companies engaging in telephone marketing. It also proscribes limitations on the use of telephone marketing, including, for instance, limiting the time of day for marketing calls, requiring the caller to

provide an opt-out of future calls and limiting the use of pre-recorded messages. There are no consent or opt-out requirements for sending marketing materials through postal mail. In addition, with the growing prevalence of telemarketers using spoofed caller IDs, the FCC is becoming more aggressive with its enforcement of the Truth in Caller ID Act. Furthermore, several states maintain an independent DNC list and regulations in which telemarketers must comply.

It is noted that the FTC, which regulates deceptive practices, has brought enforcement actions relating to the transmission of marketing emails or telemarketing calls by companies who have made promises in their publicly posted privacy policies that personal information will not be used for marketing purposes. Additionally, many states apply deceptive practices statutes to impose penalties or injunctive relief in similar circumstances, or where violation of a federal statute is deemed a deceptive practice under state law. Finally, recent comprehensive state data privacy laws, including in California, Virginia, Colorado, Utah and Connecticut, offer consumers an opt-out of sale, disclosure or processing of personal information in relation to targeted advertising or profiling.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Potentially, depending on if the entity sending the marketing is subject to jurisdiction in U.S. court and if the recipient is within the U.S.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The FTC, FCC, and the Attorneys General of the states are active in enforcement in this area.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such

lists?

Yes. However, the purchaser of the list should correlate it with the national DNC list and the purchaser's email opt-out lists. Some states forbid the sale of email addresses of individuals who have opted out of receiving marketing emails, and some forbid the sale of information obtained in connection with a consumer's purchase transaction.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The penalties under the CAN-SPAM Act can reach as high as US$51,744 per email. The penalties under the TCPA are US$500 per telephone call/text message violation, US$1,500 for each wilful or knowing violation and additional civil forfeiture fees with a penalty of up to US$10,000 for intentional violations (based on the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, passed in 2019), plus fines that can reach US$16,000 for each political message or call sent in violation of the Act. Once a consumer's telephone number has been registered on the DNC registry for 31 days, DNC laws prohibit a business from calling it. The business can be fined up to US$11,000 per call by the New York Department of State, as well as by the FTC and FCC. By way of example, the FTC and the attorneys general of several states obtained a judgment of US$280 million in 2017 for a company's repeated violation (involving over 66 million calls) of the TCPA, the FTC's Telemarketing Sales Rule and state law. Similarly, in March 2021, the FCC issued a US$225 million fine – the largest in the history of the agency – against telemarketers based in Texas for violations of the TCPA and the Truth in Caller ID Act in connection with approximately 1 billion robocalls.

Many states have their own deceptive practices statutes, which impose additional state penalties where violations of federal statutes are deemed to be deceptive practices under the state statute.

11. Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The federal Computer Fraud and Abuse Act has been used to assert legal claims against the use of cookies for behavioural advertising, where the cookies enable "deep packet" inspection of the computer on which they are placed. At least two states, California and Delaware, require disclosures to be made where cookies are used to collect information about a consumer's online activities across different websites or over time. The required disclosure must include how the operator responds to so-called "do not track" signals or other similar mechanisms. In addition, the CCPA's broad definition of "sale" (which includes when a consumer's personal information is made available for collection by third-party cookies for monetary "or other valuable consideration") and "sharing" (which encompasses the collection of data for use in cross contextual advertising), imposes obligations on businesses to provide certain notice and choice mechanisms (e.g., opt out) to consumers.

In addition, the FTC Act and state deceptive practices acts have underpinned regulatory enforcement and private class action lawsuits against companies that failed to disclose or misrepresented their use of tracking cookies. One company settled an action in 2012 with a payment of US$22.5 million to the FTC, and in 2016 agreed to pay US$5.5 million to settle a private class action involving the same conduct. In 2022, one company settled with the California Attorney General for US$1.2 million for failing to disclose to consumers that it was selling their personal information by making it available to third-party advertisers via online cookie trackers.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, as well as state surveillance laws, may come into play where cookies collect information from the computer on which they are placed

and report that information to the entity placing the cookies without proper consent.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes, the FTC has brought regulatory enforcement actions against companies that failed to disclose or misrepresented their use of cookies, as well as those companies that engaged in surveillance advertising without disclosing the practice or obtaining consent (for sensitive data). The California Attorney General has also initiated regulatory investigations for violations of the CCPA rules on "selling" and "sharing" personal information that came about through the use of cookies, which in one instance, resulted in a settlement with the California Attorney General for US$1.2 million.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Maximum fines are not set by statute.

12. Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The U.S. does not currently place restrictions on the transfer of personal data to other jurisdictions (but see question 19.2 discussing the Executive Order requesting new legislation regarding bulk data transfers to "countries of concern").

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance

of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

This is left to the discretion of the company, as the U.S. does not place restrictions on the transfer of personal data to other jurisdictions. With respect to receiving data from abroad, the European Commission adopted an adequacy decision for the EU–U.S. Data Privacy Framework (DPF), providing a mechanism to comply with data protection requirements when transferring personal data from the EU to the U.S. A business may transfer data from the U.S. to the EU if the business self-certifies to the Department of Commerce that it complies with the DPF Principles. Other mechanisms to govern data transfers from the EU to the U.S. – e.g., the use of standard contractual clauses (SCCs) or binding corporate rules – remain valid.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

No such registration/notification is required.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Transfers of personal data to other jurisdictions do not require a transfer impact assessment.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

On March 25, 2022, the U.S. and the European Commission announced that they had reached an agreement in principle to replace the Privacy Shield Framework with a new data transfer framework, the DPF. Under this framework, the U.S. has committed to strengthen privacy and civil liberties safeguards governing signals intelligence activities, establish a multi-layer redress mechanism including an independent Data Protection Review Court available to EU citizens, and enhance oversight. On October 7, 2022, President Biden signed an Executive Order, "Enhancing Safeguards for United States Signals Intelligence Activities", intending to incorporate these commitments. In 2023, the European Commission released an adequacy decision concerning the proposed framework.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The FTC has expressed "commitment to vigorous enforcement" of the DPF Principles. A business need not use SCCs if the business self-certifies to the Department of Commerce that it complies with the DPF Principles.

13. Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The federal Whistleblower Protection Act of 1989 protects federal employees, and some states have similar statutes protecting state employees. Public companies subject to the Sarbanes-Oxley Act also are required to have a whistle-blower policy, which must be approved by the board of directors, and create a procedure for receiving complaints from whistle-blowers.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting generally is permitted. Rule 10A-3 of the Securities Exchange Act of 1934, for example, requires that audit committees of publicly listed companies establish procedures for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.

14. CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV must comply with federal and state criminal voyeurism/eavesdropping statutes, some of which require signs to be posted where video monitoring is taking place, restrict the use of hidden cameras, or prohibit videotaping altogether if the location is inherently private (including places were individuals typically get undressed, such as bathrooms, hotel rooms and changing rooms). Litigation has been instituted alleging that CCTV may also violate biometrics laws such as the BIPA. For example, in 2022 a doorbell camera provider faced allegations that cameras recording passers-by without consent violates the BIPA.

14.2 Are there limits on the purposes for which CCTV data may be used?

There generally are no restrictions on the use of lawfully collected CCTV data, subject to a company's own stated policies or labour agreements.

15. Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee privacy rights, like those of any individual, are based on the principle that an individual has an expectation of privacy unless that expectation has been diminished or eliminated by context, agreement, notice or statute. Monitoring of employees generally is permitted to the same extent as it is with the public, including when the employer makes clear disclosure regarding the type and scope of monitoring in which it engages, and subject to generally applicable surveillance laws regarding inherently private locations as well as employee-specific laws such as those regarding the privacy of union member activities.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent and notice rights are state-specific, as is the use of hidden cameras. When required or voluntarily obtained, employers typically obtain consent for employee monitoring through acceptance of employee handbooks, and may provide notice by appropriately posting signs. Furthermore, the CCPA provision exempting employee personal information expired in 2023, with employee personal information now treated like consumer personal information under the CCPA.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

The National Labor Relations Act prohibits employers from monitoring their employees while they are engaged in protected union activities.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes. As a general matter, employers are entitled to monitor employees' attendance in the office. Particular forms of monitoring could be prohibited depending on the manner and circumstances of the processing. For instance, the BIPA prohibits employers from processing employees' biometric data without consent.

16. Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

In the consumer context, the FTC has stated that a company's data security measures for protecting personal data must be "reasonable", taking into account numerous factors, to include the volume and sensitivity of information the company holds, the size and complexity of the company's operations, and the cost of the tools that are available to address vulnerabilities. Certain federal statutes and certain individual state statutes also impose an obligation to ensure security of personal information. For example, the GLBA and HIPAA impose security requirements on financial services and covered healthcare entities (and their vendors). In 2021, the FTC announced its revisions to its Safeguards Rule under the GLBA with major updates taking effect in December 2022. The updated rule requires highly prescriptive safeguards including a written incident response plan, penetration testing and vulnerability assessments, encryption of customer information and multi-factor authentication, among other safeguards. Some states impose data security obligations on certain entities that collect, hold or transmit limited types of personal information. For example, the NYDFS adopted regulations in 2017 that obligate all "regulated entities" to adopt a cybersecurity programme and cybersecurity governance processes. The regulations also mandate reporting of cybersecurity events, like data breaches and attempted infiltrations, to regulators. Covered entities include those banks, mortgage companies, insurance companies and cheque-cashers otherwise regulated by the NYDFS. Enforcement of the NYDFS regulation began in early 2021. In

2022, the NYDFS announced a consent order against a company that was subject to four cybersecurity incidents. The company agreed to pay a US$5 million monetary penalty, to surrender its insurance provider licences and to stop selling insurance to New York residents. In 2023, the NYDFS adopted final amendments to its Cybersecurity Requirements for Financial Services Companies, which expanded the type of activity that would be considered a violation of the Cybersecurity Requirements and imposed additional requirements relating certification, risk assessments and governance.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

At the federal level, other than breach notification requirements pertaining to federal agencies themselves, the HIPAA requires "Covered Entities" to report impermissible uses or disclosures that compromise the security or privacy of protected health information to the HSS. Under the Privacy Rule, if the breach involves more than 500 individuals, such notification must be made within 60 days of discovery of the breach. Information to be submitted includes information about the entity suffering the breach, the nature of the breach, the timing (start and end) of the breach, the timing of discovery of the breach, the type of information exposed, safeguards in place prior to the breach and actions taken following the breach, including notifications sent to impacted individuals and remedial actions. In 2022, the U.S. enacted the Cyber Incident Reporting for Critical Infrastructure Act. This law requires companies considered part of the U.S. critical infrastructure to report substantial cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency of the U.S. Department of Homeland Security within 72 hours and to report ransomware payments within 24 hours.

While not specifically a data breach notification obligation, the Securities and Exchange Act and associated regulations, including Regulation S-K, require public companies to disclose in filings with the SEC when material events, including cyber incidents, occur. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarise and report information that is required to be disclosed in SEC filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective. In 2023, the SEC adopted rules requiring disclosures regarding material cybersecurity incidents within four business days after a materiality determination, as well as specific disclosures about public companies' cybersecurity risk management and governance in its annual disclosures.

Some state statutes require the reporting of data breaches to a state agency or Attorney General under certain conditions. The information to be submitted varies by state but generally includes a description of the incident, the number of individuals impacted, the types of information exposed, the timing of the incident and the discovery, actions taken to prevent future occurrences, copies of notices sent to impacted individuals, and any services offered to impacted individuals, such as credit monitoring. The NYDFS also requires a Covered Entity to notify the NYDFS no later than 72 hours from a determination that a Cybersecurity Event has occurred.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

At the federal level, the HIPAA requires covered entities to report data breaches to impacted individuals without unreasonable delay, and in no case later than 60 days. Notice should include a description of the breach, to include: the types of information that were involved; the steps individuals should take to protect themselves, including who they can

contact at the covered entity for more information; as well as what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches. For breaches affecting more than 500 residents of a state or jurisdiction, covered entities must provide local media notice, in addition to individual notices.

As of May 2018, all 50 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have statutes that require data breaches to be reported, as defined in each statute, to impacted individuals. These statutes are triggered by the exposure of personal information of a resident of the jurisdiction, so if a breach occurs involving residents of multiple states, then multiple state laws must be followed. Most statutes define a "breach of the security of the system" as involving unencrypted computerised personal information, but some states include personal information in any format. Triggering personal information varies by statute, with most including an individual's first name or first initial and last name, together with a data point, including the individual's Social Security Number, driver's licence or state identification card number, financial account number or payment card information. Some states include additional triggering data points, such as date of birth, mother's maiden name, passport number, biometric data, employee identification number or username and password. The standard for when notification is required varies from unauthorised access to personal information, to unauthorised acquisition of personal information, to misuse of or risk of harm to personal information. Most states require notification as soon as is practical, and often within 30 to 60 days of discovery of the incident, depending on the statute. The information to be submitted varies by state but generally includes a description of the incident, the types of information exposed, the timing of the incident and its discovery, actions taken to prevent future occurrences, information about steps individuals should take to protect themselves, information resources and any services offered to impacted individuals, such as credit monitoring.

16.4 What are the maximum penalties for personal data security breaches?

Penalties are statute- and fact-specific. Under the HIPAA, for example, monetary fines can range from US$100 to US$50,000 per violation (or per record), with a maximum penalty of US$1.75 million per year for each violation. By way of example, in 2020, the HHS and the Attorneys General of 42 states entered into a US$39.5 million settlement with a health insurer in relation to a data breach affecting the health records of over 79 million individuals. Marking the current high point for enforcement, a company agreed to pay a record penalty of at least US$575 million, and potentially up to US$700 million in a data breach settlement reached with the FTC, the CFPB, 48 states, the District of Columbia, and the Commonwealth of Puerto Rico.

17. Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

The U.S. does not have a central data protection authority. As such, the enforcement powers of the regulators will depend on the specific statute in question. Some laws only permit federal government enforcement, some allow for federal or state government enforcement, and some allow for enforcement through a private right of action by aggrieved consumers. Whether the sanctions are civil and/or criminal depends on the relevant statute. For example, HIPAA enforcement permits the imposition of civil and criminal penalties. While the HIPAA's civil remedies are enforced at the federal level by the HHS, and at the state level by Attorneys General, the U.S. Department of Justice (DOJ) is responsible for criminal prosecutions under the HIPAA. At the state level, the CPPA has the power to enforce consumer rights and business obligations under the CPRA.

a. **Investigative Powers:** Depending on the applicable data protection laws, regulators in the U.S. may have the authority to conduct investigations into potential violations of data protection requirements.

b. **Corrective Powers:** Depending on the applicable data protection laws, regulators in the U.S. may have the authority to correct non-compliance actions of businesses through injunctive relief or under consent orders.

c. **Authorisation and Advisory Powers:** Depending on the applicable data protection laws, regulators in the U.S. will often provide a method for businesses to consult with the regulators for additional and specific guidance.

d. **Imposition of administrative fines for infringements of specified GDPR provisions:** This is not relevant for our jurisdiction.

e. **Non-compliance with a data protection authority:** Depending on the applicable data protection laws, non-compliance with a data protection authority will generally attract renewed or additional enforcement against the business.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The U.S. does not have a central data protection authority. Enforcement authority, including whether a regulator may ban a particular processing activity, is specified in the relevant statutes. For example, 18 states have adopted the Insurance Data Security Model Law developed by the National Association of Insurance Commissioners. Among other things, these laws empower state insurance commissioners to issue cease-and-desist orders pertaining to data processing violations in the insurance industry, and even to suspend or revoke an insurance institution's or agent's licence to operate. The FTC may also prohibit a particular company from engaging in a particular processing activity through a negotiated consent decree as part of a settlement.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

In the U.S., this depends on the relevant statutory enforcement mechanism and the agency conducting the enforcement measures. The FTC, for example, in addition to publishing on its website all of the documents filed in FTC cases and proceedings, publishes an annual summary of key data privacy and data security enforcement actions and settlements, which provides guidance to businesses on its enforcement priorities. Similarly, the HHS publishes enforcement highlights, summarises the top compliance issues alleged across all complaints and, by law, maintains a website that lists mandatorily reported breaches of unsecured protected health information affecting 500 or more individuals. By way of an example, in 2022, the FTC entered into a consent decree that required an online marketplace to destroy improperly obtained or unnecessary data, limit future data collection, and implement an information security programme. Such requirements are commonplace in FTC consent decrees.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Extraterritorial enforcement of a U.S. law would depend on a number of factors, including whether the entity is subject to the jurisdiction of the U.S. courts, the impact on U.S. commerce and the impact on U.S. residents, among other factors.

18. E-discovery / Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

When made pursuant to Mutual Legal Assistance Treaties, information requests are typically processed through the DOJ, which works with the local U.S. Attorney's Office and local law enforcement, prior to review by a

federal judge and service on the U.S. company. In addition, under the Clarifying Lawful Overseas User of Data Act, businesses may also receive requests for electronic communications, including personal data within its possession, custody or control directly from foreign governments and agencies that maintain agreements with the U.S., without regard to where the business stores such data.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

This is not applicable in our jurisdiction.

19. Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

In 2023, the FTC continued its aggressive approach to enforcement with regard to data privacy and cybersecurity, with emphasis on artificial intelligence, children and teens, health and other sensitive data.

For example, in one landmark case in 2023, the FTC announced a joint proposed settlement of its enforcement action against a telehealth and prescription drug retailer for allegedly sharing sensitive personal information with advertising companies and platforms without notice to or authorisation from its customers. Under this order, the company is permanently prohibited from sharing users' health information with advertisers. The order also marked the first time the FTC has brought an enforcement action under the Health Breach Notification Rule (HBNR). The FTC is also considering amendments to the HBNR.

In addition, in March 2023, the FTC finalised a settlement with a video game company requiring the company to refund consumers US$245

million for charging them through the use of "dark patterns" or without obtaining affirmative consent. The FTC also brought several other enforcement actions, including action alleging: that a security camera company allowed employees and contractors to access private videos; that tax preparation firms solicited loan borrowers using information collected for tax preparation services; that a technology company improperly prevented parents from deleting children's data; that the use of facial recognition technology could be an unfair or deceptive practice; and that a genetic testing firm left user data unprotected, misled users about their ability to delete data and retroactively changed its privacy policy without consumer notice.

In addition, in December 2023, the SEC obtained nearly US$5 billion in financial remedies, its second-highest amount ever (after 2022). With this recent, historically high level of enforcement actions, the SEC has focused its efforts on individuals, barring over 100 people from serving as officers or directors for public companies.

State Attorneys General also played a key role in the U.S. data privacy enforcement environment under specific U.S. state laws in 2023. The Washington Attorney General announced a nearly US$40 million settlement with a technology company based on allegations that the company collected location data even for consumers who disabled their location history or turned off location access. In February 2024, the Connecticut Attorney General released a report highlighting its enforcement efforts under its new state data privacy law.

In early 2024, the California Attorney General announced an "investigative sweep" to inspect the compliance of "popular streaming apps and devices" with the CCPA provisions regarding opt-out mechanisms. The California Attorney General stated that businesses that sell or share consumer personal information must offer "an easy mechanism for consumers who want to stop the sale of their data". As noted above, the CCPA's definition of a data sale is expansive and includes any exchange of data for consideration, not just a payment. For

its part, the CPPA announced an enforcement sweep for the data privacy practices of connected vehicle (CV) manufacturers and related CV technologies. In early 2024, a California appellate court overturned a state trial court's ruling delaying the CPPA's authority to enforce certain regulations under the CPRA. Further, the California Attorney General announced its second settlement under the CCPA where it fined a food delivery Company US$375,000, among other penalties, for its sale of customer personal information.

Other state regulators, such as the NYDFS, were also active. In 2024, the NYDFS required a title insurer to pay US$1 million for alleged violations of state cybersecurity regulations for failure to ensure "full and complete implementation" of its cybersecurity policies and procedures in advance of a data breach that resulted in the exposure of customers' non-public information.

Class action litigation under the BIPA persisted in 2023; courts recognised some limitations. An Illinois federal judge dismissed a class action against a cloud storage vendor who stored biometric information on behalf of a third party which itself registered and scanned employee fingerprints for an employer. The cloud storage vendor did not take an "active step" toward collecting biometric information. Courts also took broad views of the BIPA's "general health care exemption", allowing the exception for a virtual try-on tool for sunglasses and for fingerprints taken prior to donating plasma. Texas and New York also brought enforcement actions under those states' biometric privacy laws.

Finally, 2023 saw a surge of privacy litigation at the state level brought under state wiretap laws that impose liability on website operators and service providers. These lawsuits, asserted in nine different states but primarily in California and Pennsylvania, claim, among other things, that the use of conventional website and web-analytic tools such as website session replays, chatbots and pixels violate wiretapping and eavesdropping state law provisions. Over 100 lawsuits were filed in 2023 alone and this trend is likely to continue in 2024.

19.2 What "hot topics" are currently a focus for the data protection regulator?

We anticipate that the following topics will remain hot over the next year: state-level consumer data privacy laws and regulations as more states move laws through their legislatures with an emphasis on consumer right controls in the absence of a federal law; consideration of comprehensive data privacy and artificial intelligence legislation by federal legislatures; use of dark patterns on consumers; business consideration and implementation of data minimisation techniques; issues relating to the collection, use and sharing of children's data; issues surrounding the consent to collect and use biometric information; issues surrounding the privacy and security of healthcare data; consumers' access to financial relief and other remedies when their data protection rights are violated, even in the absence of a showing of harm; issues surrounding AdTech and "surveillance" advertising; issues relating to automated decision making fuelled by artificial intelligence and machine learning; a continued focus by legislators and regulators alike on cybersecurity issues, particularly in the wake of data breaches and ransomware attacks involving significant technology vendor software and industrial operations; and targeting of cryptocurrency and digital assets such as non-fungible tokens by cybercriminals.

In addition, transfers of bulk data have come to the forefront, particularly with regard to transfer to jurisdictions perceived as impacting consumer safety, privacy and national security. Specifically, on February 28, 2024, President Biden signed Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern" (the EO). The EO calls for the DOJ to promulgate regulations to prevent the large-scale transfer of sensitive personal data and U.S. Government-related data to "countries of concern". Among other things, rulemaking proposed for the EO would require businesses and individuals to apply both for general and specific licences for sending bulk data to countries of concern that would otherwise be barred under regulations proposed by the DOJ.

Production Editor's Note

This chapter has been written by a member of ICLG's international panel of experts, who has been exclusively appointed for this task as a leading professional in their field by **Global Legal Group**, ICLG's publisher. ICLG's in-house editorial team carefully reviews and edits each chapter, updated annually, and audits each one for originality, relevance and style, including anti-plagiarism and AI-detection tools. This chapter was copy-edited by **Maya Tyrrell**, our in-house editor.