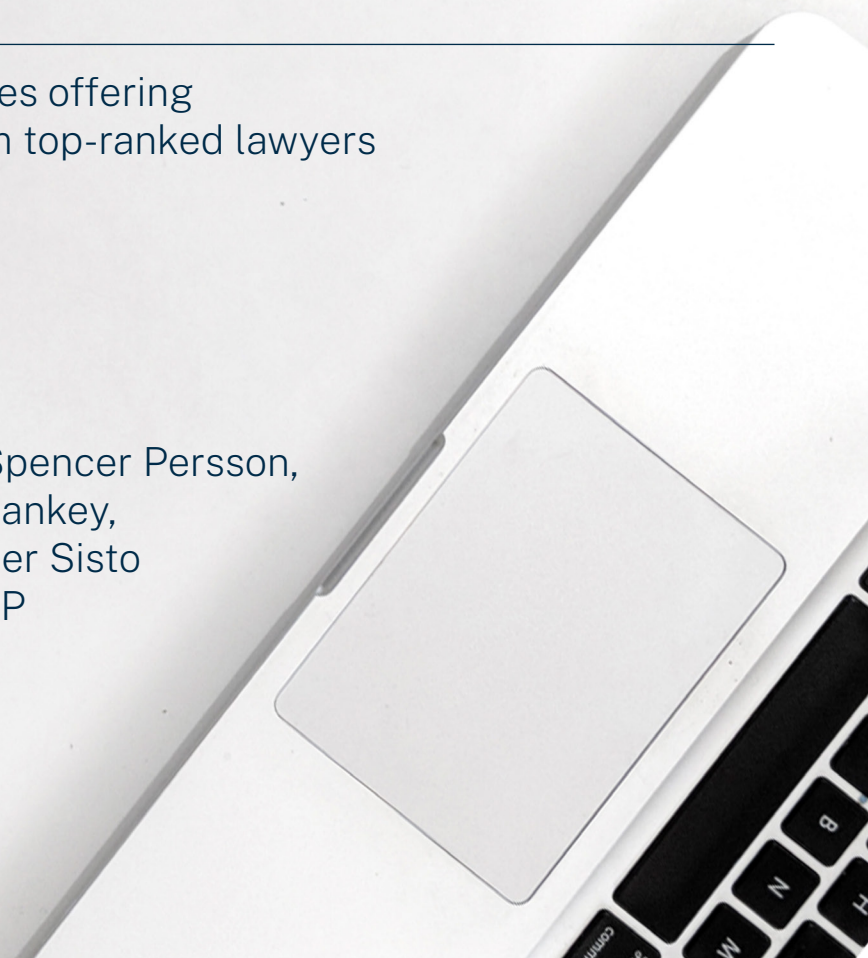
Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

Definitive global law guides offering
comparative analysis from top-ranked lawyers



USA: Law & Practice

Nancy Libin, David Rice, Spencer Persson,
Michael Borgia, Robert Stankey,
Kara Trowell and Alexander Sisto
Davis Wright Tremaine LLP

USA

Law and Practice

Contributed by:
Nancy Libin, David Rice, Spencer Persson, Michael Borgia, Robert Stankey, Kara Trowell and Alexander Sisto
Davis Wright Tremaine LLP

Contents

Contributed by: Nancy Libin, David Rice, Spencer Persson, Michael Borgia, Robert Stankey, Kara Trowell and Alexander Sisto, **Davis Wright Tremaine LLP**

Davis Wright Tremaine LLP (DWT) was founded on a simple principle: to provide clients with high-value legal services customised to their specific business challenges and objectives. Today, DWT is a national, full-service law firm with nearly 600 attorneys representing clients throughout the United States and around the world. It boasts offices across the United States, including in Chicago, Culver City, Los Angeles, New York, Portland, San Francisco, Seattle and Washington, DC, as well as in Anchorage, Bellevue, Richmond, Sacramento and Silicon Valley. The firm has nationally recognised teams serving the healthcare, technology, communications, media, financial services, energy and hospitality industries, each supported by the depth and strength of its core legal functions of business transactions, litigation, intellectual property, real estate and employment.

Authors

Nancy Libin is chair of the privacy and security practice at Davis Wright Tremaine, and helps clients comply with a wide range of sector-specific federal privacy laws, such as the Children's Online Privacy Protection Act, state privacy laws and the EU General Data Protection Regulation. A former chief privacy and civil liberties officer of the US Department of Justice, and counsel to then-Senator Joe Biden on the Senate Judiciary Committee, Nancy brings a three-dimensional understanding of law, policy and strategy that enables her to help clients effectively participate in legislative activity and government proceedings and understand regulatory trends.

David Rice leverages more than 20 years of experience in privacy and security to guide clients through compliance with rapidly multiplying and complex laws in a multi-jurisdictional environment. Drawing on his extensive knowledge of the full spectrum of federal, state and international privacy and data protection laws, David advises clients regarding a wide range of difficult privacy questions, and helps them understand and manage risk. David is a member of the Washington State Bar Association and co-chair of the Federal Communications Bar Association's Pacific Northwest Chapter.

Contributed by: Nancy Libin, David Rice, Spencer Persson, Michael Borgia, Robert Stankey, Kara Trowell and Alexander Sisto, **Davis Wright Tremaine LLP**

Spencer Persson is an experienced litigator with Davis Wright Tremaine's privacy, security and technology group, where he represents clients in data privacy matters and consumer class actions. Throughout his career as a litigator, Spencer has regularly secured verdicts and favourable settlements for his clients, which include technology companies, retailers, manufacturers, entertainment companies, insurers, healthcare providers and financial service providers (among others). Spencer has been practising for over two decades, and is a member of the Los Angeles County Bar Association.

Michael Borgia draws on nearly two decades of experience as outside counsel, in-house counsel at a global technology consultancy, and a cybersecurity consultant to deliver solutions that are practical, business-forward and tech-savvy. A veteran incident-response professional, Mike has led investigations of and responses to hundreds of security incidents, from ransomware attacks to trade secret theft and sophisticated nation-state hacking campaigns. He has represented clients in complex investigations by federal and state authorities as well as multi-state attorneys general, following data breaches and other types of cybersecurity and data privacy incidents.

Robert Stankey focuses on telecommunications, media and technology law. He has an in-depth knowledge of privacy and telecom regulation in the USA, Europe and Asia. He counsels clients on commercial contracts and legal compliance matters. A former senior in-house lawyer in the USA and Europe, he practised with two international firms in London and is qualified to practice in the USA and the UK. Bob has been practising for nearly four decades, and is a member of the International Technology Law Association.

Kara Trowell helps clients across a spectrum of industries – including the technology, entertainment, advertising, retail and telecommunications sectors – on business-oriented strategies for compliance with federal, state and international privacy laws. Kara regularly teams up with her clients' legal, technology, HR and information security professionals to address privacy issues; develop and strengthen privacy and information governance programmes, practices and procedures; and help them understand how the latest legal and regulatory developments may have an impact on their business. Kara has nearly a decade of experience and is a member of the International Association of Privacy Professionals.

Contributed by: Nancy Libin, David Rice, Spencer Persson, Michael Borgia, Robert Stankey, Kara Trowell and Alexander Sisto, **Davis Wright Tremaine LLP**

Alexander Sisto helps clients proactively comply with US state, federal and international privacy regulations by drafting privacy policies and agreements as well as international data transfer mechanisms. Alex advises clients on AI governance issues, including engaging with regulators regarding rapidly developing US and international AI regulations. Alex also helps prepare for and respond to cybersecurity incidents, including data breaches, by managing post-breach investigations and advising on US and international reporting obligations. Alex has been practising for nearly a decade, and is a member of the International Association of Privacy Professionals.

Davis Wright Tremaine LLP

920 5th Ave #3300
Seattle, WA 98104
USA

Tel: +1 206 622 3150
Web: www.dwt.com

Contributed by: Nancy Libin, David Rice, Spencer Persson, Michael Borgia, Robert Stankey, Kara Trowell and Alexander Sisto, **Davis Wright Tremaine LLP**

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

Data privacy is regulated in the US by various legal authorities, including the US Constitution, federal and state statutes and regulations, and local law.

US Constitution

The First Amendment, in some circumstances, protects people's right to speak or engage in other protected activities anonymously, and the Fourth Amendment requires law enforcement, when investigating a crime, to obtain a warrant, issued by a judge or magistrate based on a showing of "probable cause" that specifically identifies the places to be searched or the things to be seized.

Federal Statutes

Federal statutes regulate data privacy in certain sectors, and the Federal Trade Commission (FTC), which is the principal federal privacy regulator, also has authority to bring enforcement actions related to data privacy and security.

General consumer protection

The FTC uses Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce, to bring enforcement actions against companies with regard to their privacy and security practices.

Financial institutions and monetary affairs

The Fair Credit Reporting Act (FCRA) governs data used to evaluate consumers for extension of credit, employment, insurance and certain other matters.

The Gramm-Leach-Bliley Act (GLBA) and the Safeguards Rule govern protection of non-public consumer personal information and disclosures by certain financial institutions to third parties.

The Right to Financial Privacy Act imposes certain data privacy obligations on particular financial institutions.

Children's privacy

The Children's Online Privacy Protection Act (COPPA) regulates online collection, use and disclosure of personal information from children under the age of 13, and generally requires notice and verifiable parental consent before doing so.

Education privacy

The Family Educational Rights and Privacy Act governs access, use and disclosure of "education records" and students' personally identifiable information.

Health information

The Health Insurance Portability and Accountability Act (HIPAA) regulates health information privacy and security, but applies only to certain "covered entities" and, in some cases, covered entities' service providers, known as "business associates".

The Confidentiality of Substance Use Disorder Patient Records rule regulates substance use disorder records generated by certain federally conducted or assisted programmes.

Communications and media

The Cable Act prohibits cable operators' disclosure of personally identifiable information of subscribers to cable and other services, unless authorised by the Act or by specific court orders

with notice to subscribers, including the opportunity for subscribers to contest certain orders.

The Video Privacy Protection Act (VPPA) prohibits providers of physical and digital audio-visual materials from disclosing information identifying video rentals or usage without specific advance subscriber consent, subject to limited exceptions.

The Electronic Communications Privacy Act (ECPA) includes the following:

- the Stored Communications Act requires a specific legal process (eg, subpoena, court order or warrant) for governmental entities to access certain customer information, records, communications content and wireless caller tower location data, or National Security Letters to obtain information for national security investigations;
- the Wiretap Act requires a specific legal process – generally a warrant – for governmental access to live communications (voice and online content); and
- the Pen Register/Trap and Trace Act generally requires governmental entities to obtain a court order to access live outbound and inbound subscriber call connection information (metadata).

The Telephone Consumer Protection Act protects consumers from unwanted "robocalls" and text messages made using auto-diallers and/or an artificial, synthetic or prerecorded voice.

The CAN-SPAM Act protects consumers from unwanted unsolicited commercial emails.

The Communications Act prohibits telephone companies from disclosing certain data about consumers' telecommunications services, communications metadata and bills without customer consent, subject to limited exceptions.

Driver's licence information

The Driver's Privacy Protection Act prohibits states from selling information acquired from individuals while issuing driver's licences and automobile registrations.

Information in computer systems

The Computer Fraud and Abuse Act prohibits unauthorised access, or exceeding authorised access, to certain computer systems.

Biometric data

The FTC can bring enforcement actions under the FTC Act against commercial entities regarding their handling of biometric data. The FTC defines biometric data to include facial, eye or fingerprint data that identifies individuals.

Government access to personal information

For information held by the federal government:

- the Privacy Act governs the collection, use and disclosure of personally identifiable information by federal agencies; and
- the Freedom of Information Act generally requires government agencies to disclose certain information upon request, but exempts certain information if disclosure would be an unwarranted invasion of privacy.

For law enforcement and intelligence community access to personal information:

- the ECPA (see above) imposes specific duties on law enforcement in obtaining wiretaps, access to stored communications content and subscriber records, and for national security investigations;

- the Privacy Protection Act requires special showing by law enforcement to gain access to materials held by the press; and
- the Foreign Intelligence Surveillance Act establishes special procedures for electronic surveillance of, and obtaining records and information relating to, persons considered to be "agents of a foreign power" in the context of national security investigations.

State Statutes

In the absence of comprehensive federal privacy legislation, states began to enact their own omnibus consumer privacy statutes. States have also enacted laws that protect particular types of sensitive personal information (eg, biometric information) and information in certain industry sectors.

State General Privacy Laws

20 US states have enacted broad consumer privacy laws. These laws provide similar consumer rights and data controller and processor obligations.

California Consumer Privacy Act (CCPA)

The CCPA applies to for-profit entities doing business in California that determine the purposes and means of data processing and meet the jurisdictional threshold – ie, that:

- annually have revenue of over USD26.625 million;
- buy, sell or share the personal information of 100,000 or more California residents; or
- derive more than 50% of revenue from selling or sharing California consumers' personal information.

These entities are "businesses", similar to "controllers" under the GDPR. Businesses must do the following, among other things, subject to exceptions:

- disclose how they collect and otherwise process consumers' personal information;
- comply with consumers' requests to exercise their rights;
- enter into contracts with service providers and contractors (equivalent to "processors" under the GDPR) to define and limit the service provider's ability to use personal information for purposes other than providing services to the business;
- enter into contracts with third parties to/with whom they sell or share personal information;
- implement reasonable data security measures;
- recognise browser settings indicating a consumer's request to opt out of sales or sharing of personal information;
- limit the collection, use and disclosure of personal information to what is necessary for the disclosed purposes;
- refrain from selling or "sharing" the personal information of consumers who the business has actual knowledge of being under 16 years of age, unless the parent (if the consumer is under 13 years of age) or consumer (if the consumer is at least 13 but under 16 years of age) consents; and
- ensure that the consent consumers provide is freely given, specific, informed and unambiguous.

Under the CCPA, consumers (California residents) have rights to do the following:

- confirm that a regulated CCPA business is processing their personal information;
- access and obtain a copy of that personal information in a portable format;
- correct their inaccurate personal information;

- delete their personal information;
- opt out of data "sales" (exchanges of their personal information with third parties for monetary or other valuable consideration);
- opt out of data "sharing" (providing their personal information to a third party for cross-context behavioural advertising);
- limit the use and disclosure of their sensitive personal information; and
- opt out of profiling performed by automated decision-making technology that has significant legal or similar effects.

The California Privacy Protection Agency (CPPA) and the California attorney general enforce the CCPA. The CPPA has authority to promulgate implementing regulations. The CCPA provides a limited private right of action for consumers in the event of a data breach caused by inadequate security safeguards.

In addition to the CCPA, the California Online Privacy Protection Act requires operators of websites and online services that collect personally identifiable information from California residents to post a privacy policy that contains certain information, and the California "Shine the Light" Law requires businesses that have disclosed certain personal information of California consumers to third parties for those third parties' own direct marketing purposes to give consumers the right to receive information about those disclosures and those third parties.

The CCPA compared with other state privacy statutes

While the CCPA is like other state privacy statutes in many respects, there are some important differences, as follows.

The CCPA protects the personal information of employees and individuals in an employment and business context, whereas the other state privacy laws apply only to personal information in a personal or household context.

Except in the few cases noted below, other state laws do not use the amount of a company's annual revenue as a jurisdictional threshold. Instead, with a couple of exceptions, they use the number of state residents whose personal data an entity collects or the revenue the entity derives from the sale of personal information.

While the CCPA uses the terms "business" and "service provider" (and "contractor"), the other state laws use the terms "controller" and "processor", which are roughly equivalent to the same terms in the GDPR. All state privacy laws use the term "third party" to describe entities that are none of these, however.

The CCPA gives consumers the right to limit the processing of their sensitive personal information that is used to infer characteristics about them, while most other states require entities to obtain consent from consumers before processing their sensitive personal information. States generally define "sensitive" personal data to include information revealing:

- race or ethnic origin;
- religious beliefs;
- citizenship or immigration status;
- genetic data;
- biometric data;
- physical or mental health diagnosis; and
- sexual orientation.

Some states add additional categories to the foregoing, such as precise geolocation, philosophical beliefs, sex life, union membership and – in California and Colorado – neural data (among others).

Thus far, only the laws of California, Colorado, Florida and New Jersey authorise rulemaking to implement their privacy laws.

While most state laws expressly exempt entities covered by sector-specific privacy laws (eg, financial institutions regulated under the GLBA), the CCPA provides exemptions that exempt the information, rather than the entities, governed by sector-specific statutes.

The CCPA has a limited private right of action for certain data breaches, whereas none of the other state privacy laws has a private right of action.

These other state laws, with a few exceptions, provide the same rights to consumers and impose the same obligations on controllers, though each has its own unique provisions, as described below.

Colorado

The Colorado Privacy Act (CPA) uses as a jurisdictional threshold the amount of consumers' personal data processed annually (at least 100,000 or more, or 25,000 if the controller derives revenue or consumers receive a discount, from the sale of personal data). Colorado controllers include non-profit entities. The CPA requires controllers to perform a data protection assessment for processing personal information that may cause a heightened risk of harm, such as targeted advertising. Colorado controllers must have an appeals process for consumers who object to how their requests are handled.

Connecticut

The Connecticut Data Privacy Act (CTDPA), as amended, has applicability thresholds like the CPA. The CTDPA does not apply to non-profits, however. The CTDPA prohibits targeted advertising to, and the sale of personal data of, consumers who the controller has actual knowledge of or wilfully disregards as being 18 years' old without consent (parental consent is required for children under 13).

Virginia

The Virginia Consumer Data Protection Act (VCDPA) is like the CPA, but does not apply to non-profits. The VCDPA also gives controllers a right to cure non-compliance before enforcement.

Utah

The Utah Consumer Privacy Act (UCPA) applies to businesses that both:

- have annual revenues of USD25 million; and
- either annually process the personal information of 100,000 or more Utah consumers or derive more than 50% of their revenue from the sale of their personal data, or annually process the personal data of more than 25,000 Utah consumers.

Also, the UCPA:

- does not require data protection assessments;
- does not provide a right to opt out of profiling; and
- gives consumers the right to opt out of sensitive data processing rather than requiring controllers to obtain their opt-in consent for such processing.

Iowa

The Iowa Consumer Data Protection Act (IACDPA) defines a "sale" as an exchange of personal data with a third party for monetary consideration only, and, like the Utah law, it gives consum-

ers the right to opt out of (not opt in to) sensitive data processing.

Nebraska

The Nebraska Data Privacy Act (NDPA) applies to entities that:

- do business in Nebraska or produce products or services targeted at Nebraska residents;
- process or engage in the sale of personal information; and
- are not small businesses under the federal Small Business Administration.

The NDPA does not apply to non-profits.

Delaware

The Delaware Personal Data Privacy Act (DPDPA) largely follows the Colorado model but applies to controllers that control or process the personal data of at least 35,000 Delaware consumers. The DPDPA applies to non-profits and has no HIPAA-entity level exemption.

New Hampshire

The New Hampshire Expectation of Privacy statute is similar to Delaware, except that it does not apply to non-profits.

New Jersey

The New Jersey Data Privacy Act (NJDPA) roughly follows the Colorado model, except that:

- controllers must obtain opt-in consent to process personal information when the controller has actual knowledge or wilfully disregards that the consumer is a child who is at least 13 years of age and younger than 17 years of age, when that processing is for the purpose of targeted advertising, a sale or profiling;
- the NJDPA defines "sensitive" data to include potentially all of a consumer's financial information (to the extent that it is not covered by GLBA); and
- personal information processed solely for the purpose of completing a payment transaction is excluded from the personal data needed to meet the jurisdictional threshold.

Oregon (effective 1 July 2024 generally, and 1 July 2025 for non-profits)

The Oregon Consumer Privacy Act (OCPA) follows the Colorado model, and, like the CPA, applies to non-profit entities, with some exceptions. The OCPA has no GLBA or HIPAA entity-level exemptions. The OCPA gives consumers the right to obtain the names of specific third parties to which the controller has disclosed the consumers' personal information, but the controller can respond by disclosing the names of the specific third parties to which it has disclosed personal data generally. Oregon requires controllers to obtain consent (from parents, for children under 13) before selling or using the personal information of children under 16 for targeted advertising.

Texas

The Texas Data Privacy and Security Act (TDPSA), like the Nebraska law, has no per-consumer collection threshold and instead applies to entities that:

- conduct business in Texas or produce a product or service consumed by Texas residents;
- process or engage in the sale of personal data; and
- are not small businesses as defined by the federal Small Business Administration.

Controllers that sell sensitive personal data must prominently disclose the following: "NOTICE: We may sell your sensitive personal data."

Similarly, controllers that sell biometric personal data must provide the following: "NOTICE: We may sell your biometric personal data."

Montana

The Montana Consumer Data Privacy Act (MCDPA) prohibits the sale of personal data of consumers who the controller has actual knowledge of being under 16 and the use of their personal information for targeted advertising without consent (parental consent is required for consumers under 13 years of age).

Minnesota (effective 31 July 2025 generally, and 31 July 2029 for post-secondary institutions)

The Minnesota Consumer Data Privacy Act (MCDPA) is like the Colorado law, but gives broader rights to consumers who are subject to profiling by automated decision-making technology in certain circumstances. Such consumers have the right to:

- challenge the result of such profiling;
- be informed of the reasons for the decision;
- learn what the consumer could have done or could do in the future to achieve a different result; and
- review the information used in the profiling, with possible rights of correction and re-evaluation.

The MCDPA, like the Oregon law, also gives consumers the right to a list of specific third parties to whom the controller has disclosed their personal information, or a list of all specific parties to which the controller has disclosed personal information generally.

Indiana (effective 1 January 2026)

The Indiana Consumer Data Protection Act (INCDPA) is similar to the Virginia law and defines a data sale as the exchange of personal data for monetary consideration only.

Kentucky (effective 1 January 2026)

The Kentucky Consumer Data Protection Act (KCDPA) also resembles the Virginia law. The KCDPA provides a right to cure, does not require controllers to recognise browser opt-out signals, and defines a "sale" as the exchange of personal data for monetary consideration only.

Tennessee (effective 1 July 2025)

The Tennessee Information Protection Act (TIPA) largely resembles the Virginia law by, among other things, adopting the narrow definition of a data sale as the exchange of data for "valuable monetary consideration". The TIPA is unique in allowing controllers and processors to assert an affirmative defence to claims that their data practices are inadequate if they adopt and comply with a written privacy programme that "reasonably conforms" to the National Institute of Standards and Technology privacy framework or a similar framework.

Rhode Island (effective 1 January 2026)

The Rhode Island Data Transparency and Privacy Protection Act (RI-DTPPA) has the same general applicability threshold as Delaware (35,000 consumers).

Maryland (effective 1 October 2025)

The Maryland Online Data Privacy Act (MODPA) has the same low applicability thresholds as Delaware and similar consumer rights and controller obligations, but it also includes some unique provisions that make compliance more difficult – for example, as follows.

- Biometric data means data generated by automatic measurements of biological char-

acteristics that *can be* used (not just data that *is* used) to identify an individual.
- Consumer health data, which is also sensitive data, includes physical or mental health status (not just a diagnosis) and data related to gender-affirming care and reproductive or sexual health care.
- The MODPA prohibits controllers, regardless of consumer consent, from:
  (a) processing sensitive data unless strictly necessary to provide a service or product requested by the consumer;
  (b) selling sensitive personal data (although consumer-directed disclosures are permitted); or
  (c) collecting personal data, unless necessary and proportionate for providing a product or service to the consumer.
- The MODPA prohibits the use of personal information of anyone who the controller knew *or should have known* was under the age of 18 for sales or targeted advertising.

Florida

The Florida Digital Bill of Rights (FDBR) applies to only a few very large companies – ie, those that have USD1 billion or more in annual revenue *and* obtain at least 50% of their revenue from digital advertisement sales, operate an app store or other digital distribution platform with at least 250,000 applications, or operate a consumer smart speaker. Only a handful of companies meet these requirements.

The FDBR otherwise has controller obligations and consumer rights that resemble those of the Virginia law, with some exceptions, including the following.

- As under the Texas law, controllers that sell sensitive personal data or biometric data must provide consumers with these disclosures: "NOTICE: We may sell your sensitive personal data", or "NOTICE: We may sell your biometric personal data". Both disclosures need to be prominent and in the same location as the controller's privacy policy.
- The FDBR also prohibits controllers and processors from collecting data when a voice-activated device is not in active use by a consumer, unless the consumer expressly authorises collection.

Sector-Specific State Privacy Statutes: Health Data

The Washington My Health My Data Act

The Washington My Health My Data Act (MHMD) is not a generally applicable state privacy law but is broad enough to affect many companies that process data not typically regarded as health data.

- The MHMD applies to consumer health data (CHD), which is personal information that is linked or reasonably linkable to and identifies a covered consumer's past, present or future physical or mental health status.
- Consumers are Washington residents and people whose data is "collected" – broadly defined to include data that is "processed" – in Washington.
- Regulated entities must disclose their collection of CHD and must obtain consent before collecting, sharing or selling CHD. The process for obtaining consent for selling CHD is onerous.
- Consumers have rights similar to those under the general state privacy laws, such as the right to access their CHD.
- "Any violation" of the MHMD is a per se violation of the Washington Consumer Protection Act and is enforced by attorney general *and* through a private right of action under the

Washington Consumer Protection Act, unlike state consumer privacy laws.

Nevada

Nevada's Consumer Health Data Law (NVCHDL) is like Washington's MHMD, except that it has no private right of action.

Sector-Specific State Privacy Statutes: Biometric Data

Three US states (Illinois, Texas and Washington) have laws that govern the collection, use, disclosure and storage of biometric data. Such data typically includes retina or iris scans, fingerprints, voiceprints and scans of hand or face geometry. All of these statutes impose notice and consent obligations on covered entities, although specific requirements vary.

Illinois

The Biometric Information Privacy Act (BIPA) prohibits collection of biometric data without specific advance notice and express consent in writing. It prohibits the selling, leasing or trading of, or profiting from, biometric data under any circumstances, without any exception for consent. The BIPA also uniquely requires companies to provide a publicly available policy that includes a retention schedule and destruction guidelines for biometric data. The BIPA provides a private right of action allowing for the recovery of statutory and actual damages.

Texas

The Capture or Use of Biometric Identifier Act (CUBI) prohibits the capture of biometric data for a commercial purpose without advance notice and express consent. The CUBI prohibits the sale, lease or other disclosure of biometric data to third parties unless one of several very narrow exceptions applies.

Washington

Washington's law prohibits the enrollment of biometric data for a commercial purpose – ie, for marketing products that are unrelated to the initial transaction in which the data was collected – without advance notice, consent or a mechanism that notifies consumers of the subsequent use of the biometric data for a commercial purpose.

Other Sector-Specific State Privacy Statutes

State privacy laws also cover additional issues, such as the following.

Wiretapping/electronic eavesdropping

All 50 states prohibit surreptitious interception of private electronic communications and monitoring or recording of private in-person and electronic communications without the consent of at least one of the participants to the communication, subject to exceptions. 12 states require consent of all participants.

Student privacy laws

Most states have enacted laws that limit how operators of websites, applications and online services that market and provide their products and services to K-12 schools and school districts collect, use and disclose the personal information of students.

Data breach notification and data security

All US states and most US territories have enacted data breach notification laws. These laws generally require entities that own, license or maintain personal information of state residents to notify individuals in the event of unauthorised access to acquisition of personal information about those individuals. Such laws typically apply to a core set of personal information, such as:

- individuals' names in combination with Social Security number, driver's licence number or other state ID number; and
- financial account or payment card numbers in combination with any required information (eg, security code) that permits access to an individual's account.

Some such laws also apply to certain types of medical and health insurance information, certain usernames and passwords, and biometric data. Most of these laws also require notification to the state attorney general or other state agency.

Many states also have enacted data security laws, which generally require entities to protect personal information from unauthorised access, acquisition or other misuse. Generally, these requirements are broadly stated and require entities to maintain "reasonable" security measures. Some of these laws also specifically require contractual obligations to impose reasonable security measures on any third parties to which an entity discloses personal information, and to securely delete personal information when no longer needed.

Several states (eg, Massachusetts, New York and Oregon) have more detailed requirements. Those state laws require various administrative, technical and physical safeguards for personal information, such as:

- information security policies;
- third-party risk management;
- access controls;
- incident response procedures;
- patch management;
- employee training; and
- secure deletion.

Health information confidentiality

States generally govern the confidentiality of health information through:

- general medical privacy laws governing healthcare providers, and potentially other types of entities (eg, health insurers);
- confidentiality laws specific to certain conditions or treatments; and
- broad consumer privacy laws governing health data that falls outside HIPAA (see the discussion above concerning Washington's MHMD and similar Nevada law).

Some states (notably California) also prohibit certain healthcare providers from responding to in-state or out-of-state warrants for data on use of reproductive healthcare services.

Data brokers

Four states – California, Vermont, Texas and Oregon – require data brokers to register with state agencies. Definitions vary, but generally "data brokers" are businesses that collect and sell or license the personal data of individuals with whom the business does not have a direct relationship. In addition, California's Delete Act directs the CPPA to develop a mechanism that enables consumers – with one request – to delete personal information held by all data brokers registered with the state.

Disposal of records containing personal information

Most states have enacted laws that require businesses to securely destroy or dispose of personal information that is no longer needed. Acceptable methods typically include shredding or burning paper records and other media and altering electronic records to make them unreadable.

State unfair or deceptive practices statutes
State consumer protection statutes that prohibit companies from engaging in unfair or deceptive acts or practices are often used to protect consumers' privacy interests.

State privacy torts
Most states recognise common law privacy torts such as "intrusion upon seclusion" and "publication of private facts". (Some states have codified these torts in statutes.) The elements of these torts vary, but in general, if an intrusion into private spaces or affairs, or a publication of the private facts, would be "highly offensive to a reasonable person", the person harmed may be able to sue for monetary damages.

Local Level Overview
Smaller jurisdictions within states, such as counties, townships and cities, have enacted local laws to address specific privacy issues.

The New York City Biometric Identifier Information Act has two distinct components. The law:

- requires commercial establishments to disclose on a sign at the entrance of the business their collection, use, storage and sharing of customers' biometric data; and
- prohibits the selling, leasing or trading of, or otherwise profiting from, the transaction of biometric data.

Violations are enforceable by a private right of action.

More than a dozen local governments have banned or significantly limited use of facial recognition by government agencies. The City of Portland, Oregon was the first to extend such regulation to private entities.

1.2 Regulators
A number of regulators at the federal and state level have investigative and enforcement authority. Some also have authority to promulgate rules to implement privacy laws.

Federal Trade Commission (FTC)
The FTC requires entities under its jurisdiction to:

- abide by the representations that they make in their privacy policies or other public statements regarding their data privacy practices;
- refrain from engaging in unfair practices (such as failing to disclose the sharing of personal data with third parties); and
- maintain adequate data security safeguards.

In addition, the FTC is responsible for protecting children's privacy rights under COPPA and has certain enforcement responsibilities under other federal privacy statutes, including HIPAA.

Other Federal Agencies
Other federal agencies have authority to enforce privacy laws and regulations under their respective jurisdictions. Examples include the following.

- The Consumer Financial Protection Bureau (CFPB), which is generally responsible for enforcing privacy laws in the context of transactions with financial institutions and under the FCRA, and can bring enforcement actions against companies that engage in unfair, deceptive or abusive acts or practices. The CFPB also administers and enforces Regulation P, which implements data privacy requirements for financial institutions under the GLBA. As later discussed, it also enforces the Personal Financial Data Rights rule, which provides consumers with certain rights to

control the sharing and use of their personal financial information.
- The Department of Health and Human Services Office for Civil Rights, which is the primary enforcer of the HIPAA privacy, security and breach notification regulations (for HIPAA civil enforcement, see also **State Agencies** below).
- The Department of Justice (DOJ), which may bring criminal prosecutions for knowingly obtaining or disclosing protected health information in violation of HIPAA.
- The Federal Communications Commission (FCC), which is responsible for enforcing (along with the DOJ) the provisions of the Communications Act that protect the privacy and security of customer account information and telecommunications metadata.
- The Securities and Exchange Commission (SEC), which requires publicly traded companies to disclose material information regarding their operations and risks, including those related to data privacy and security. A recently enacted SEC rule requires public companies to disclose material cybersecurity incidents within four business days of determining that the incident is material. The SEC also promulgates GLBA-related customer data privacy rules for certain financial institutions.

State Agencies

State attorneys general and/or state consumer protection agencies generally have authority to enforce state privacy laws and regulations, and some state consumer protection laws give consumers a private right of action. State attorneys general also have authority to enforce certain federal privacy laws, such as COPPA and HIPAA, when violations of those laws have an impact on state residents. Finally, California is the first state to establish a standalone privacy regulator, the California Privacy Protection Agency (CPPA).

1.3 Enforcement Proceedings and Fines

Regulators (such as the FTC) generally initiate enforcement proceedings when a particular issue comes to the agency's attention, either from press reports (for example, reports of data breaches), complaints from private parties or inquiries from other governmental entities.

Proceedings generally begin with a formal request for information, such as through a civil investigative demand, directing entities to answer questions, or a less formal (but legally binding) subpoena or "letter of inquiry". These requests can require recipients to answer questions and produce records relevant to the inquiry.

Once the data-gathering phase is complete, the agency determines whether to initiate a formal enforcement proceeding. Prior to initiating a formal proceeding, most agencies will discuss the matter with the potential target to determine if a settlement can be reached. Agencies – and the FTC in particular – enter into settlements more frequently than they litigate formal enforcement proceedings. Settlements often include agreed-upon payments in the nature of fines.

1.4 Data Protection Fines in Practice

Fines for alleged privacy violations vary. The FTC has negotiated fines as high as USD5 billion against a company that violated the privacy-related consent order it was operating under, as well as fines in the hundreds of millions of dollars against companies for alleged COPPA violations. Smaller fines are more common, however. For example, AT&T recently agreed to pay USD13 million to the FCC to settle claims that it failed to adequately protect consumer account information and call metadata, and Verizon and

AT&T were recently fined USD47 million and USD57 million respectively for violations of their obligation to protect the location information of their wireless customers.

State regulators impose fines as well. In August 2022, the California Attorney General announced a USD1.2 million settlement with Sephora, a retailer of personal care and beauty products, resolving allegations that Sephora had not disclosed that it was selling consumers' personal information and that it had not recognised consumers' opt-out preference signals regarding the sale of their personal information.

In February 2024, the California Attorney General entered into a USD375,000 settlement with DoorDash regarding DoorDash's alleged sale of consumer personal information without providing notice or an opt-out opportunity.

1.5 AI Regulation

States have enacted several AI-specific laws.

The Utah Artificial Intelligence Policy Act requires deployers of generative AI technology to provide notice that the consumer is interacting with generative AI technology:

- upon request from the consumer;
- if the interaction involves activity regulated by the Utah Division of Consumer Protection; and
- whenever the technology is engaged in an activity requiring a licence from the Utah Department of Commerce.

The Colorado Artificial Intelligence Act (CAIA), effective on 1 February 2026, imposes notice, disclosure, risk mitigation and opt-out requirements on deployers and developers of high-risk AI systems, and requires some disclosures for all AI systems that engage with consumers. High-risk systems are those that interact with consumers and that make, or are a substantial factor in making, consequential decisions regarding employment, insurance, housing, credit, education and healthcare.

The California Generative Artificial Intelligence Training Data Transparency Act, effective on 1 January 2026, will require developers of generative AI systems made publicly available to California consumers to publicly post disclosures regarding data used to train those systems, including whether the datasets include personal information.

California's "unlawful use of bots" law requires notice that a bot is being used to communicate or interact with another person in California online in order to incentivise a purchase of goods or influence a vote in an election. Bots are defined as automatic online accounts where posts or actions are not "the result of a person".

1.6 Interplay Between AI and Data Protection Regulations

In addition to AI-specific regulations, the general consumer protections in federal and state general privacy laws as described in **1.1 Overview of Data and Privacy-Related Laws** also regulate AI technology through their broad scope.

FTC

The FTC's jurisdiction over unfair or deceptive acts or practices applies to AI technology just as it does to other services and industries. Examples of FTC enforcement and priorities related to AI technology include:

- requiring entities to implement measures to prevent harm before and after deploying AI technology;

- preventing AI-related deepfakes;
- preventing surreptitious and retroactive changes to privacy policies, to justify the use of personal data to train AI models; and
- directing developers and deployers of AI technology to disclose in their privacy policies the sources of their training data.

State General Privacy Laws

State privacy and consumer protection laws also have an impact on the development and deployment of AI technology to the extent that models are trained on personal information or are fine-tuned with personal information. Among others, issues that arise include:

- honouring consumer requests to exercise their privacy rights when it may be difficult or even impossible to isolate personal information in an AI training database or model;
- providing sufficient transparency of personal data collection and processing;
- preventing undisclosed secondary uses of personal data; and
- managing consumer rights with respect to automated decision-making technology that profiles consumers in connection with decisions that have a significant impact on them.

2. Privacy Litigation

2.1 General Overview

The privacy litigation landscape has expanded greatly in the past 18 months to include new theories relating to the use of third-party vendors to augment companies' online presence and the collection and sharing of certain data with those vendors. These relationships have spawned new theories relating to video-viewing habits of consumers and the reinterpretation of wiretapping claims. Meanwhile, data breach litigation continues, along with new collective actions that seek to use companies' terms of service against them.

Wiretapping, Pen Registers, and Tap and Trace Litigation

Much of the so-called "wiretapping" litigation that became pervasive in 2024 invokes the California Invasion of Privacy Act (CIPA), which was originally enacted in the 1960s and was designed to prohibit the interception or recording of telephone calls without consent. Plaintiffs have brought claims under CIPA to allege that the use of third-party vendors to operate chat functions, improve website functionality or provide advertising metrics to the company somehow constitutes an illegal wiretap. Plaintiffs have also claimed that a related provision designed to allow law enforcement to install pen registers or trap and trace devices on suspected criminals' phone lines applies to any website's procurement of an IP address – a far-fetched notion considering that an exchange of IP addresses is required for internet operability.

Plaintiffs argue that these violations of CIPA result in statutory damages of USD5,000 per violation. While companies have had some success in defeating these claims at the pleading stage, often the cases are settled for nuisance value and before an appellate decision is issued that could foreclose the claims moving forward. One set of enterprising plaintiffs alleged that customer voice-authentication systems used by financial institutions violated CIPA's provisions that prohibit examining or recording a person's voiceprint or voice stress patterns to determine "the truth or falsity of statements made by such person".

Biometrics

More than 2,000 cases have been litigated under the Illinois BIPA. Challenges to "fingerprint" timekeeping systems, facial or voice recognition authentication systems, and in-store security systems have been subject to multiple asserted claims, some resulting in "ruinous" damage awards prompting significant legislative amendments to BIPA in 2024.

The Texas State Attorney General has brought and settled multiple claims against online platforms under CUBI for alleged unconsented use and processing of biometric data and unauthorised disclosures.

Children's Privacy Laws

Social media and technology companies have worked together to challenge, on First Amendment grounds, state laws designed to restrict the use of algorithms to deliver content to minors, obtaining injunctions in some instances to delay implementation and enforcement. The cases are still developing, with litigation continuing and some states choosing to modify the statutes in a manner more likely to survive legal challenges.

2.2 Recent Case Law

Data Breach Litigation

Consumer data breach class actions continue to cause companies headaches long after the incident has passed. While defendants have some success at the pleading stage and in defeating motions for class certification, the settlement value of cases involving statutory damages under statutes such as the CCPA has climbed higher, with plaintiffs typically insisting on non-reversionary funds with cash awards to persons covered by the statutory claims. Plaintiffs have been willing to hold out for greater settlements based in large part on the reluctance of defendants to litigate these matters, especially where they have insurance coverage. Moreover, plaintiffs' recent success in obtaining favourable class certification orders over the past year has further increased the value of these cases, even if those orders were not as broad as plaintiffs requested.

VPPA Litigation

Websites of all sorts that link to video content and use third-party vendors to assist with website operations or analytics continue to find themselves in litigation, facing allegations that they have violated the VPPA. Like the claims under CIPA, these VPPA claims assert that websites that link to video content and share certain information with business partners (usually by "pixels") violate the VPPA. Companies had enjoyed some amount of success in obtaining dismissals at the pleading stage, but the US Court of Appeals for the Second Circuit's broad definition of what constitutes a "consumer" and "subscriber" under the statute will ensure that the filings continue.

Internet Privacy Litigation

The US Court of Appeals for the Sixth Circuit overturned an FCC reclassification of internet access service as a "telecommunications" service that would have subjected internet service providers (ISPs) to potentially expansive privacy rules, drastically limiting their collection, use and processing of internet users' data.

2.3 Collective Redress Mechanisms

The USA has always been the legal standard bearer in allowing collective or class actions, and that continues to be true in ongoing privacy litigation matters. Attorneys representing consumers have added another arrow to their quiver in bringing privacy claims over the past few years, turning mandatory arbitration provisions and class action waivers contained in the compa-

nies' terms of service against them. Specifically, by assembling hundreds or thousands of consumers through online advertising campaigns in bringing CIPA, VPPA or other privacy claims with statutory damages attached, these attorneys have used the threat of pursuing mass arbitrations to force exorbitant settlements based on the prohibitive cost of paying for individualised arbitrations – costs that largely fall on the company. Even with claims that are dubious on the merits, settlement often makes sense because reaching the merits requires advancing significant fees to the arbitral forum.

While companies have been fighting back by modifying their terms to allow for grouped or batched arbitrations where mass claims are threatened, the arbitral bodies have been slow to adjust to plaintiffs' increased willingness to weaponise the arbitration process, and courts that have reviewed the new provisions have expressed skepticism relating to enforceability.

3. Data Regulation on IoT Providers, Data Holders and Data Processing Services

3.1 Objectives and Scope of Data Regulation

The USA has not enacted a federal law like the EU Data Act, which aims to foster innovation and support the provision of services by making data more accessible and usable. Federal agencies and state legislatures have been active in this area, however. For instance, the CFPB recently issued its Personal Financial Data Rights rule (also frequently referred to as the "Open Banking" rule or the 1033 rule after the section of the Consumer Financial Protection Act that it implements), which requires certain financial institutions to make transaction data available to consumers (and third parties acting with consumers' authorisation) in a standardised format that would enable use of that data by other entities in the financial services ecosystem. In addition, state privacy laws typically give consumers the right to obtain their personal data free of charge and in a format that enables portability so that they can transfer their personal data to another service. These laws are designed to foster both competition and innovation in the digital economy.

Regarding regulations governing internet of things (IoT) providers, the USA has focused more on the security of IoT devices than on the ability of such devices to make data available for use by others. For instance, the IoT Cybersecurity Improvement Act of 2020 directed the National Institute of Standards and Technology (NIST) to develop standards and guidelines for the federal government on the appropriate use and management of IoT devices "owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices". While this legislation regulates federal government procurement practices, it will nonetheless have an impact on the consumer marketplace as manufacturers that sell such devices to the federal government adjust their practices according to NIST guidelines.

In addition, two states – California and Oregon – have passed legislation mandating that manufacturers of IoT devices sold in those states ensure, among other things, that such devices have "reasonable security features" to protect the device and any information "from unauthorised access, destruction, use, modification or disclosure". Other states have proposed similar legislation.

3.2 Interaction of Data Regulation and Data Protection

In the USA, some laws and regulations designed to foster competition in the digital information ecosystem also impose data privacy obligations, to ensure that such data will be protected even as the data is made available for new products and services. For instance, as previously noted, the CFPB's Personal Financial Data Rights rule seeks to promote competition among various providers in the financial technology ecosystem by giving consumers the right – free of charge – to request the transfer of their personal financial data in usable format to third parties and to allow third parties to access such data with consumer authorisation. By requiring certain financial institutions, defined as "data providers" (what would be "data holders" under the EU Data Act), to make this data available, consumers may be able to switch between financial institutions more easily, potentially increasing competition and improving service offerings.

The CFPB's rule is also intended to spur innovation in the fintech marketplace by enabling greater interoperability among banks and various fintech providers. At the same time, the rule also imposes privacy and data protections, such as requiring data providers and third parties to limit the purposes for which consumer data is used and disclosed, and prohibiting the sale of consumer data or its use for targeted advertising and cross-selling. The rule also imposes various data security obligations of the GLBA on data providers and third parties.

Similarly, the state laws that give consumers the right to obtain their personal data in a portable and readily usable format, when technically feasible, are privacy laws that require companies to give consumers certain privacy rights and protections. These laws also generally impose data minimisation requirements on companies, limiting the amount of personal data that they can process to what is necessary, reasonable and proportionate for the purposes disclosed to the consumer. These data minimisation requirements may limit the amount of personal information that is ultimately available for transfer to or access by another entity.

3.3 Rights and Obligations Under Applicable Data Regulation

Data-processing services, including cloud service providers and similar service providers, are subject to the laws and regulations described in the foregoing sections and that apply generally to controllers and processors of personal information. To that end, consumers have the right under state privacy laws to request that data-processing service providers give them a portable and readily usable copy of their personal data, or otherwise enable the transfer of such data directly to another provider.

3.4 Regulators and Enforcement

While the CFPB has authority to enforce the Personal Financial Data Rights rule, there has been no enforcement of said rule as of this article's publication, since the first of several compliance dates is not until 1 April 2026. The CFPB's enforcement authority flows from the Consumer Financial Protection Act, which allows the CFPB to file an action in federal court or by initiating an administrative adjudication proceeding in response to violation of its regulations.

4. Sectoral Issues

4.1 Use of Cookies

Unlike in the EU, businesses are not required – except in limited circumstances – to obtain opt-in consent from consumers in the USA before

allowing cookies to collect their personal data. (The one exception is for trackers present on websites or platforms displaying or allowing access to video content.) Therefore, cookie, banners are not required in the USA, although businesses increasingly use them. Instead, US state laws require businesses to provide consumers with a mechanism to opt out of the disclosure of their personal information to third-party cookies when such disclosures are for monetary or other valuable consideration (called a "sale" under many state privacy laws) or for targeted advertising (ie, advertising based on consumers' online activities over time and across unaffiliated websites).

Most state privacy laws *do* require businesses to obtain opt-in consent from consumers before allowing third-party cookies to collect certain sensitive personal data or before "selling" personal data (ie, making such data available to certain types of third-party cookies) collected from consumers known to be minors or before allowing third-party cookies to collect such data for targeted (or personalised) advertising.

4.2 Personalised Advertising and Other Online Marketing Practices

As previously noted, comprehensive state privacy laws generally require controllers to give consumers the opportunity to opt out of the processing of their personal information for "targeted advertising". State laws generally define "targeted advertising" as "displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across non-affiliated websites, applications or online services to predict consumer preferences or interests".

The CCPA uses different terminology but similarly requires businesses to give consumers the chance to opt out of "cross-context behavioural advertising", which it defines as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications or services, other than the business, distinctly branded website, application or service with which the consumer intentionally interacts". The CCPA is slightly more restrictive because it treats entities as a single "business" only if they are under common control *and* share common branding. Therefore, an entity that uses personal information obtained from a consumer's activity across its differently branded affiliates' websites for targeted advertising may need to provide the consumer with a mechanism to opt out of such advertising.

State privacy laws generally require controllers to provide an opt-out link in the footer of their website homepages, and many state privacy laws require controllers to recognise browser-based opt-out signals that consumers can configure to signal their requests to opt out of sales and for sharing of personal data for targeted or cross-context behavioural advertising.

As previously noted, some states require opt-in consent to process the personal data of minors for targeted advertising, and most states with comprehensive privacy laws require opt-in consent to process sensitive personal data. Therefore, controllers will need to obtain opt-in consent before engaging in targeted advertising in some circumstances.

4.3 Employment Privacy Law

The USA does not have a comprehensive federal employee privacy law, but an employer's handling of employees' personal information may be subject to sector-specific federal and state laws designed to protect the confidentiality of certain

information (eg, FCRA, the Americans with Disabilities Act, BIPA (biometrics) and various state personnel file laws). There are also federal and state constitutional, statutory and common law protections for privacy in the employment context, as follows.

If the employer is a government entity:

- courts have applied the Fourth Amendment and required a warrant for searching an employee's "private" office and files; and
- the Wiretap Act and Stored Communications Act will in some cases apply to employer monitoring of employee conversations, telephone calls and electronic communications of a personal nature – some states have analogous laws that may have broader scope, include additional requirements or prohibitions, and impose harsher sanctions than their federal counterparts.

If the employer is a private entity, the Fourth Amendment does not apply. However, the following should be noted.

- A handful of state constitutions, including California and Alaska, specify a right to privacy that has been interpreted to apply in the employment context.
- The state privacy torts may apply to employer conduct that unreasonably intrudes on an employee's privacy. The common law invasion of privacy claims most common in the employment context are intrusion upon seclusion, public disclosure of private facts, and false light publication.
- Some states have laws regulating specific employee conduct or employee privacy in certain information and circumstances, such as:
  - (a) personnel file laws that govern access to and inspection of employee records;
  - (b) surveillance laws that set forth requirements and limitations on video or biometric monitoring in the workplace;
  - (c) specific laws that protect an employee's personal online account and activities;
  - (d) laws that govern an employer's use of GPS, location and vehicle tracking devices; and
  - (e) laws that protect employees' off-duty activities.
- Some states require employers to notify employees before electronically monitoring their phone calls, emails or internet usage. New York law requires employees' written acknowledgement of the notice.
- Federal law and some state laws (California) generally prohibit the use of polygraph devices by private employers, and both federal and state laws apply to employer monitoring of private employee conversations and communications.
- Like the GDPR, the CCPA applies to the processing of personal information in the employment context and grants privacy rights that can be exercised by employees and job applicants.

In all cases, employees may have specific privacy rights established in a written employment contract.

4.4 Transfer of Personal Data in Asset Deals

Control of personal data is typically transferred between corporate entities as part of a merger, acquisition, asset purchase or other corporate transaction. In many cases, receipt of such personal data by the acquiring entity may be necessary for the acquiring entity to provide services or may have substantial value on its own (for

example, for identifying and marketing to potential or former customers).

Before a merger, acquisition or other corporate transaction is closed, the acquiring entity will typically engage in due diligence of the target (or selling) entity's data privacy and security practices. This typically involves a review of the target entity's policies and procedures, and obtaining information from the target's subject matter experts. As part of the transaction, the acquiring entity will typically receive representations and warranties from the target or selling entity related to data privacy and security.

State data privacy laws permit a target entity to transfer personal data to an acquiring entity as part of a proposed or actual merger, acquisition or other transaction without triggering a "sale" of personal data under those laws. Companies therefore need not offer consumers a right to opt out. The CCPA, however, expressly prohibits the acquiring entity from using or disclosing this personal data in a manner that is materially inconsistent with the commitments made to consumers by the target entity unless the acquiring entity provides adequate notice of the change in practices.

5. International Considerations

5.1 Restrictions on International Data Transfers

While US laws generally do not impose restrictions on the transfer of personal information outside the USA, restrictions have recently been imposed for national security reasons on transfers of certain US personal data, with a particular focus on transfers to China. While these restrictions are aimed at data brokers selling personal information to foreign governments and affiliated companies, international data transfers to governments or state-controlled entities in politically sensitive countries will need to be evaluated given the potential scope of these new measures.

For instance, the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA) prohibits data brokers from selling, licensing, renting, trading, transferring, releasing, disclosing, providing access to or otherwise making available personally identifiable sensitive data of a US individual (ie, a person residing in the USA) to any foreign adversary country or any entity controlled by a foreign adversary. Sensitive data includes government-issued identifiers, biometric information, genetic information and precise geolocation information. Such data is considered personally identifiable if it identifies or is reasonably linkable to (alone or in combination with other data) an individual or their device. Foreign adversary countries are currently defined as China, Iran, North Korea and Russia.

Most recently, the US Supreme Court upheld the Protecting Americans from Foreign Adversary Controlled Applications Act, which banned TikTok from operating in the USA, requiring that it go dark or have its controlling interest severed from Chinese control, based on national security considerations. The law was also upheld based on preventing China's control over a communications platform that allowed it to collect sensitive personal data associated with 170 million US TikTok users.

Separately, new DOJ regulations that cover a wide range of transactions restrict foreign access to sensitive US data by "countries of concern" and other "covered entities", including private persons and entities that are subject to the control or jurisdiction of "countries of concern". The regulations implement the Biden

administration's Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern. The restrictions apply to transactions involving sensitive personal data that exceeds certain bulk volume thresholds. The current "countries of concern" are China, Cuba, Iran, North Korea, Russia and Venezuela. Sensitive personal data includes precise geolocation information, biometric identifiers, human genomic data, personal health data, personal financial data and personal identifiers (eg, names linked to advertising IDs).

5.2 Government Notifications and Approvals

The Committee on Foreign Investment in the United States (CFIUS), a division of the US Department of Treasury, can block transactions that could allow foreign adversaries access to US sensitive personal data. Indeed, in September 2022, President Biden signed the Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States (CFIUS), which, among other things, directed the CFIUS to scrutinise transactions involving sensitive personal data.

5.3 Data Localisation Requirements

There are no general localisation requirements for personal data under US law. However, sector-specific laws and regulations may have the effect of requiring certain types of information to be kept within US territory.

5.4 Blocking Statutes

See **5.2 Government Notifications and Approvals**.

5.5 Recent Developments

See **5.1 Restrictions on International Data Transfers**.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com