DATA PROTECTION LAWS OF THE WORLD

United States

DLA PIPER

UNITED STATES

Last modified 24 January 2022

LAW

United States privacy law is a complex patchwork of national, state and local privacy laws and regulations. There is no comprehensive national privacy law in the United States. However, the US does have a number of largely sector-specific privacy and data security laws at the federal level, as well as many more privacy laws at the state (and local) level.

Federal and State Privacy Laws and Regulations

Federal laws and regulations include those that apply to financial institutions, telecommunications companies, credit reporting agencies and healthcare providers, as well as driving records, children's privacy, telemarketing, email marketing and communications privacy laws.

There are also a number of state privacy and data security laws that overlap with federal law—some of these state laws are preempted in part by federal laws, but others are not. US states have also passed privacy and data security laws and regulations that apply across sectors and go beyond federal law—such as data security laws, secure destruction, Social Security number privacy, online privacy, biometric information privacy, and data breach notification laws. Generally, each state's laws apply to personal information about residents of that state or activities that occur within that state. Thus, many businesses operating in the United States must comply not only with applicable federal law, but also with a number of state privacy and security laws and regulations.

For example, California alone has more than 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act (CCPA), which introduced sweeping definitions and broad individual rights, and imposed substantial requirements and restrictions on the collection, use and disclosure of personal information. While the CCPA was the first cross-sector, comprehensive privacy law in the United States, several others have since been passed—including the California Consumer Privacy Rights Act (CPRA), which takes effect January 1, 2023 and substantially amends the CCPA, expanding consumer rights and imposing additional compliance obligations and restrictions related to the personal information about California residents. The CPRA also established a new California enforcement agency, which is expected to lead to increased enforcement.

Beyond California, both Virginia and Colorado have enacted new comprehensive state privacy laws that take effect in 2023—the Virginia Consumer Data Protection Act (effective January 1, 2023) the Colorado Privacy Act (effective July 1, 2023), respectively. While not identical, the Colorado and Virginia laws are substantially similar to each other. Further, both are also generally inapplicable to personal information collected about employees and business relationships. On the other hand, while the CPRA has some practical similarities with the Colorado and Virginia laws, it adopts definitions, requirements and restrictions that vary considerably from these laws, and also, notably, applies to personal information collected from California residents in employment and B2B contexts. More information from DLA Piper on the CCPA and related issues is available at https://www.dlapiper.com/en/us/focus/ccpa/.

In addition, a number of other US states have proposed state-level privacy legislation (including Florida, Maryland, and Oklahoma). Thus, it is highly possible that additional state-level privacy laws will be enacted in the US in 2022.

Enforcement of Unfair and Deceptive Trade Practices

In the United States, consumer protection laws, which prohibit unfair and deceptive business practices, provide another avenue for enforcement against businesses for their privacy and security practices.

At the federal level, the US Federal Trade Commission (FTC) uses its authority to protect consumers against unfair or deceptive trade practices, to take enforcement actions against businesses for materially unfair privacy and data security practices. The FTC uses this authority to, among other things, take enforcement actions and investigate companies for:

- Failing to implement reasonable data security measures
- Making materially inaccurate or misleading privacy and security statements, including in privacy policies
- Failing to abide by applicable industry self-regulatory principles
- Transferring or attempting to transfer personal information to an acquiring entity in a bankruptcy or M&A transaction, in a manner not expressly disclosed on the applicable consumer privacy policy
- Violating consumer privacy rights by collecting, using, sharing or failing to adequately protect consumer information, in violation of standards established in their prior enforcement precedents

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states. State attorneys general also sometimes work together on enforcement actions against companies for actions that broadly affect the consumers of multiple states (such as data breaches).

DEFINITIONS

Definition of personal data

Varies widely by law and regulation. The definition of personal information varies under US law. Some laws—such as data breach and security laws—apply more narrowly, to sensitive personal information, such as government identifiers, financial account information, password, biometrics, health insurance or medical information, and other information that can lead to identity fraud and theft or financial harm. On the other hand, under a number of state and federal laws, personal information broadly includes any information that identifies or is linked or reasonably linkable to an individual.

California

Under the CCPA and CPRA, personal information includes information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The definition specifically includes name, alias, contact information, government IDs, biometrics, genetic data, location data, account numbers, education history, purchase history, online and device IDs, and search and browsing history and other online activities, if such information is linked or linkable with a particular consumer or household. Under the law, consumer is broadly defined as any resident of California.

Colorado

Under the Colorado Privacy Act, personal data includes information that is linked or reasonably linkable to an identified or identifiable individual, who is a Colorado resident acting an individual or household capacity (*ie*, personal information about individuals acting in an employment or B2B context are not in scope).

Virginia

Under the Virginia Consumer Data Protection Act, personal data includes any information that is linked or reasonably linked to an identified or identifiable natural person, who is a Virginia resident acting in an individual or household capacity (*ie*, personal information about individuals acting in an employment or B2B context are not in scope).

Definition of sensitive personal data

Varies widely by sector and by type of statute.

Generally, includes personal health data, financial data, credit worthiness data, student data, biometric data, personal information collected online from children under 13, and information that can be used to carry out identity theft or fraud are considered sensitive, and subject to additional restrictions and regulations.

For example, state breach notification laws and data security laws generally apply to more sensitive categories of information, such as Social security numbers and other government identifiers, credit card and financial account numbers, passwords and user credentials, health or medical information, insurance ID, digital signatures, and/or biometrics.

California

The CPRA defines *sensitive personal information* as personal information that reveals about a consumer one or more of the following types of information, including:

- Social Security, driver's license, state identification card or passport number
- account log-in, financial account, debit card or credit card number in combination with any required security or access code, password or credentials allowing access to an account
- precise geolocation
- racial or origin, religious or philosophical beliefs, or union membership
- contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication
- genetic data
- biometric information
- health information
- information about sex life or sexual orientation

The CCPA does not define sensitive personal information.

Virginia

Under the Virginia Consumer Data Protection Act, *sensitive data* is defined as a category of personal data that includes data revealing racial or ethnic origin, religious beliefs, physical or mental health diagnosis, sexual orientation, or citizen or immigrant status, as well as processing of genetic or biometric data for identification, precise geolocation data, and personal data collected from a known child.

NATIONAL DATA PROTECTION AUTHORITY

There is no single national authority.

With some exceptions (such as for banks, credit unions and insurance companies), the FTC has jurisdiction over most commercial entities and has authority to issue and enforce federal privacy regulations (including telemarketing, email marketing, and children's privacy) and to take enforcement action to protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices.

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states.

California

The California Attorney General has the authority to enforce the CCPA and CPRA (once in force) and most California consumer privacy laws. Additionally, the CPRA establishes a new enforcement agency, the California Privacy Protection Agency (CPPA), vested with administrative power and authority to implement and enforce the CPRA.

California consumers also have a private right of action, under both the CCPA and CPRA, for certain data breaches.

Colorado

The Colorado Attorney General has the authority to enforce the CPA

Virginia

The Colorado Attorney General has the authority to enforce the VCDPA.

In addition, a wide range of sector-specific regulators, particularly those in the healthcare, financial services, telecommunications and insurance sectors, have authority to issue and enforce privacy and security regulations, with respect to entities under their jurisdiction.

REGISTRATION

There is no requirement to register databases or personal information processing activities. However, two states impose certain registration requirements on data brokers:

California

The CCPA (as amended in 2019) requires (subject to some exceptions) that data brokers register with the California Attorney General. Under the law, a "data broker" is defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. The terms "sell" and "personal information" are defined as set forth in the CCPA.

Vermont

In 2018, passed a law requiring data brokers to register with the secretary of state and adhere to minimum data security standards. Under the law a "data broker" is defined as a company that collects computerized, personal information of Vermont residents with whom the company has no direct relationship, and either sell or licenses that information.

In addition, several state laws require entities that engage in certain types of telemarketing activities to register with the state attorney general or other consumer protection agency.

DATA PROTECTION OFFICERS

With the exception of entities regulated by HIPAA, there is no general requirement to appoint a formal data security officer or data privacy officer.

Massachusetts and some other state laws and federal regulations require organizations to appoint one or more employees to maintain their information security program.

COLLECTION & PROCESSING

US privacy laws and self-regulatory principles vary widely, but generally require that a notice be provided or made available pre-collection *(eg,* in a privacy policy) that discloses a company's collection, use and disclosure practices, the related choices consumers have regarding their personal information, and the company's contact information.

Opt-in consent is required under certain circumstance to collect, use and disclose certain sensitive data, such as health information, credit reports, financial information, children's personal information, biometric data, video viewing choices, geolocation data and telecommunication usage information.

The CPA (Colorado) and VCDPA (Virginia) require a business obtain consent from consumers to collect their sensitive data.

The (federal) Children's Online Privacy Protection Act (COPPA) requires verifiable parental consent prior to the collection of any personal information from children under 13. In addition, the CCPA and CPRA require that a business obtain explicit consent prior to the sale of any personal information about a consumer that the business has "actual knowledge" is less than 16 years old, and where the consumer is less than 13 years old, express parental authorization is required. (As discussed further below, the

definition of "sale" under the CCPA is very broad and may include online advertising and retargeting activities, for example.). Under the CPRA, this concept expands to the concept of "sharing" a minor's consumer personal information (as such term is broadly defined under the CPRA).

Further, companies generally need to obtain opt-in consent prior to using, disclosing or otherwise treating personal information in a manner that is materially different than what was disclosed in the privacy policy applicable when the personal information was collected. The FTC deems such changes 'retroactive material changes' and considers it unfair and deceptive to implement a retroactive material change without obtaining prior, affirmative consent. Under the CCPA (California), which applies to individual and household data about California residents, businesses must, among other things:

- At or before collection, notify consumers of the categories of personal information to be collected and the purposes of use of such information
- Post a privacy policy that discloses
    - the categories of personal information collected, categories of personal information disclosed for a business purpose, and categories of personal information "sold" by the business in the prior 12 months
    - the purposes for which the business collects, uses and sells personal information
    - the categories of sources from which the business collects personal information
    - the categories of third parties to whom the business discloses personal information and
    - the rights consumers have regarding their personal information and how to exercise those rights
- Includes a "do-not-sell my information" link on the business's website and page where consumers can opt-out of the sale of their personal information (if applicable)
- Generally, provide at least two methods for consumers to submit CCPA requests to the business, including an online method (e.g., submission of an online form) and a toll-free number

Other California privacy laws (*eg*, the California "Shine the Light Law" and the California Online Privacy Protection Act) currently in force impose additional notice obligations, including:

- Where any personal information is disclosed to a third party for their own marketing use, a specific notice about such disclosure (*eg*, in a company's privacy policy) must be provided and accessible through a special link on their homepage. Further, the law gives California residents to request a list of the personal information and third parties to whom such information was disclosed for marketing purposes in the prior 12 months
- Whether the company honors any do-not-track mechanisms

Under US privacy law such as the CCPA, individuals have rights to request access and deletion of their personal information and to "opt out" of sales of their personal information. Under the upcoming California (CPRA), Colorado (CPA) and Virginia (VCDPA) privacy laws, consumers will have additional rights, including the right to correction of their personal information and the certain rights to opt out of sales, sharing and targeted advertising. Further, these laws require businesses to conduct data protection or risk assessments before engaging in certain higher-risk processing activities, such as processing that relates to:

- Certain unfair or intrusive profiling or targeted advertising purposes
- Selling of personal data
- Processing sensitive data

Virginia's law (VCDPA) also requires businesses to establish an internal process whereby consumers may appeal a controller's refusal to take action on a privacy request and where the appeal is denied, an online mechanism or other method by which the consumer can submit a complaint to the Colorado Attorney General

Other states impose a wide range of specific requirements, particularly in the student and employee privacy areas. For example, a significant number of states have enacted employee social media privacy laws, and, in 2014 and 2015, a disparate array of education privacy laws. In addition, there a number of sector-specific privacy laws that impose notice obligations, significantly limit permitted disclosures of personal information, and grant individuals the right to access or review records about the individual that are held by the regulated entity.

The US also regulates marketing communications extensively, including telemarketing, text message marketing, fax marketing and email marketing (which is discussed below).

TRANSFER

There are generally no geographic transfer restrictions that apply in the US, except with regard to storing some governmental records and information.

SECURITY

Most US businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (*eg*, health or financial information, telecommunications usage information, biometric data, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for such data.

For example, Massachusetts has enacted regulations that apply to any company that collects or maintains sensitive personal information (*eg*, name in combination with Social Security number, driver's license, passport number, or credit card or financial account number) on Massachusetts residents. Among other things, the Massachusetts regulations require regulated entities to have a comprehensive, written information security program and set forth the minimum components of such program, including binding all service providers who touch this sensitive personal information data to protect it in accordance with the regulations. Massachusetts law includes encryption requirements on the transmission of sensitive personal information across wireless networks or beyond the logical or physical controls of an organization, as well as on sensitive personal data stored on laptops and portable storage devices.

Some states impose further security requirements on payment card data and other sensitive personal information. In 2019, New York passed a new law (the New York "SHEILD Act") setting forth minimum security obligations for safeguarding private information. The SHIELD Act does not mandate specific safeguards but rather provides that a business will "be deemed to be in compliance" with the law if it implements a security program that includes elements set forth in the SHIELD Act.

The CCPA provides a private right of action to individuals for certain breaches of unencrypted personal information, which increases class action risks posed by data breaches.

There are also a number of other sectoral data security laws and regulations that impose specific security requirements on regulated entities – such as in the financial, insurance and health sectors. Federal financial regulators impose extensive security requirements on the financial services sector, including requirements for security audits of all service providers who receive data from financial institutions. For example, the New York Department of Financial Services (NYDFS) regulations impose extensive cybersecurity and data security requirements on licensees of the NYDFS, which includes financial services and insurance companies. The national Gramm-Leach-Bliley Act and implementing regulations require financial institutions to implement reasonable security measures.

HIPAA regulated entities are subject to much more extensive data security requirements. HIPAA security regulations apply to so-called 'covered entities' such as doctors, hospitals, insurers, pharmacies and other healthcare providers, as well as their 'business associates' which include service providers who have access to, process, store or maintain any protected health information on behalf of a covered entity. 'Protected health information' under HIPAA generally includes any personally identifiable information collected by or on behalf of the covered entity during the course of providing its services to individuals.

Internet of Things

California recently enacted the first US Internet of Things (IoT) legislation, effective January 1, 2020. Under SB 327, manufacturers of most IoT and Bluetooth connected devices will be required to implement reasonable security features 'appropriate to the nature and the function of the device and the information the device may collect, contain or transmit' and 'designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.'

BREACH NOTIFICATION

All 50 US states, Washington, DC, and most US territories (including, Puerto Rico, Guam and the Virgin Islands) have passed breach notification laws that require notifying state residents of a security breach involving more sensitive categories of

information, such as Social Security numbers and other government identifiers, credit card and financial account numbers, health or medical information, insurance ID, tax ID, birthdate, as well as online account credentials, digital signatures and/or biometrics.

Under many state laws, where more than 500 individuals are impacted, notice is must also be provided to credit bureaus. Nearly half of states also require notice to state attorneys general and / or other state officials of certain data breaches. Also, some state data breach laws impose certain (varying) notice content and timing requirements with respect to notice to individuals and to state attorneys general and/or other state officials.

Federal laws require notification in the case of breaches of healthcare information, breaches of information from financial institutions, breaches of telecom usage information held by telecommunication providers, and breaches of government agency information.

ENFORCEMENT

Various entities enforce US national and state privacy laws. Violations of privacy laws and rules are generally enforced by the FTC, state attorneys general or the regulator for the industry sector in question. Civil penalties can be significant.

In addition, individuals may bring private rights of action (and class actions) for certain privacy or security violations.

Some privacy laws (for example, credit reporting, marketing and electronic communications, video viewing history, call recording and cable communications privacy laws) may be enforced through private rights of action, which give rise to class action lawsuits for significant statutory damages and attorney's fees, and individuals may bring actions for actual damages from data breaches.

As of January 1, 2020, California law (the CCPA) now provides individuals with a private right of action and statutory damages, in the event of certain breaches of unencrypted personal information, where a business has failed to implement reasonable data security procedures (this applies to most categories of personal information under California's breach notification law) – this raises significant class action risks.

In June 2018, Ohio became the first US state to pass cybersecurity safe harbor legislation. Under SB 220, a company that has suffered a data breach of personal information has an affirmative defense if it has 'created, maintained, and complied with a written cybersecurity program that contains administrative, technical, and physical safeguards to protect personal information that reasonably conforms to an industry recognized cybersecurity framework' (*eg*, PCI-DSS standards, NIST Framework, NIST special publications 800-171, 800-53, and 800-53a, FedRAMP security assessment framework, HIPAA, GLBA).

ELECTRONIC MARKETING

The US regulates marketing communications extensively, including email and text message marketing, as well as telemarketing and fax marketing.

Email

The CAN-SPAM Act is a federal law that applies labeling and opt-out requirements to all commercial email messages. CAN-SPAM generally allows a company to send commercial emails to any recipient, provided the recipient has not opted out of receiving such emails from the sender, the email identifies the sender and the sender's contact information, and the email contains instructions on how the recipient can easily and without cost opt out of future commercial emails from the sender. The FTC and state attorneys general, as well as ISPs and corporate email systems can sue violators. Knowingly falsifying the origin or routing of a commercial email message is a federal crime.

Text Messages

Federal and state regulations apply to the sending of marketing text messages to individuals. Express consent is required to send text messages to individuals, and, for marketing text messages, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any text messaging (marketing or informational) program needs to be carefully reviewed for strict compliance with legal requirements.

Calls to Wireless Phone Numbers

Similar to text messages, federal and state regulations apply to marketing calls to wireless phone numbers. Prior express consent is required to place phone calls to wireless numbers using any autodialing equipment, and, for marketing calls, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any campaign or program that involves calls (marketing or informational) to phone numbers that may be wireless phone numbers needs to be carefully reviewed for strict compliance with legal requirements. The definition of autodialing equipment is generally considered to, broadly, include any telephone system that is capable of (whether or not used or configured storing or producing telephone numbers to be called, using a random or sequential number generator.

Telemarketing

Beyond the rules applicable to text messaging and calling to wireless phone numbers, there are federal and state telemarketing laws as well. Federal telemarketing laws apply to most telemarketing calls and programs, and state telemarketing law will apply to telemarketing calls placed to or from within that particular state. As a result, most telemarketing calls are governed by federal law, as well as the law of one or more states. Telemarketing rules vary by state, and address many different aspects of telemarketing, such as calling time restrictions, do-not-call registries, opt-out requests, mandatory disclosures, requirements for completing a sale, executing a contract or collecting payment during the call, further restrictions on the use of auto-dialers and pre-recorded messages, and record-keeping requirements. Many states also require telemarketers to register or obtain a license to place telemarketing calls.

Fax Marketing

Federal law and regulations generally prohibit the sending of unsolicited advertising by fax without prior, express consent. Violations of the law are subject to civil actions and have been the subject of numerous class action lawsuits. The law exempts faxes to recipients that have an established business relationship with the company on whose behalf the fax is sent, as long as the recipient has not opted out of receiving fax advertisements and has provided their fax number 'voluntarily,' a concept which the law specifically defines.

The law also requires that each fax advertisement contain specific information, including:

- A 'clear and conspicuous' opt-out method on the first page of the fax
- A statement that the recipient may make a request to the sender not to send any future faxes and that failure to comply with the request within 30 days is unlawful, and
- A telephone number, fax number, and cost-free mechanism to opt-out of faxes, which permit consumers to make opt-out requests 24 hours a day, seven days a week
- Violations are subject to a private right of action and statutory damages, and thus pose a risk of class action lawsuits

ONLINE PRIVACY

There is no specific federal law that *per se* regulates the use of cookies, web beacons and other similar tracking mechanisms. However, the state online privacy laws require notice of online tracking and of how to opt out of it.

Under California law, any company that tracks any personally identifiable information about consumers over time and across multiple websites must disclose in its privacy policy whether the company honors any 'Do-Not-Track' method or provides users a way to opt out of such tracking; however, the law does not mandate that companies provide consumers a 'Do-Not-Track' option. The same law also requires website operators to disclose in their privacy policy whether any third parties may collect any personally identifiable information about consumers on their website and across other third party websites, and prohibits the advertising of certain products, services and materials (including alcohol, tobacco, firearms, certain dietary supplements, ultraviolet tanning, tattoos, obscene matters, etc.). Further, given the CCPA's broad definition of personal information, information collected via cookies, online, mobile and targeted ads, and other online tracking are likely to be subject to the requirements of the law.

Further, given the broad definition of personal information under the comprehensive state privacy laws, information collected via

cookies and similar technologies is generally subject to the requirements of the law (e.g., notice and consumer rights). For example, under the CCPA a "sale" includes selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal information by one business to another business or a third party for monetary or other valuable consideration. This broad definition may sweep in certain online advertising activities -- for example, where a business permits the collection and use of information through certain third party cookies and tags on their website, in order to better target the business' ad campaigns on third party websites or in exchange for compensation from a third party ad network.

Minors

The Children's Online Privacy Protection Act and regulations (COPPA) applies to information collected automatically (*eg*, via cookies) from child-directed websites and online services and other websites, online services and third party ad networks or plug-ins that knowingly collect personal information online from children under 13. COPPA also regulates behavioral advertising to children under 13 as well as the collection of geolocation information, requiring prior verifiable parental consent to engage in such advertising or collection.

California law requires that operators of websites or online services that are directed to minors or that knowingly collect personally identifiable information from minors permit minors that are registered users of their sites to remove any content the minor has posted from the site or online service. The law does not give minors the right to remove information posted by third parties. Minors must be given clear notice on how to exercise their right to removal. Certain state privacy laws (such as the CCPA, CPA or VCDPA) also require that a business obtain explicit consent prior to selling any personal information about an individual the business has actual knowledge is under 16 years old.

Location Data

Generally, specific notice and consent in needed to collect precise *(eg,* mobile device) location information.

KEY CONTACTS

Andrew Serwin
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +1 858 677 1418
andrew.serwin@dlapiper.com

Jennifer Kashatus
Partner
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

Kate Lucente
Partner and Co-Editor, Data Protection Laws of the World
T +1 813 222 5927
kate.lucente@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.