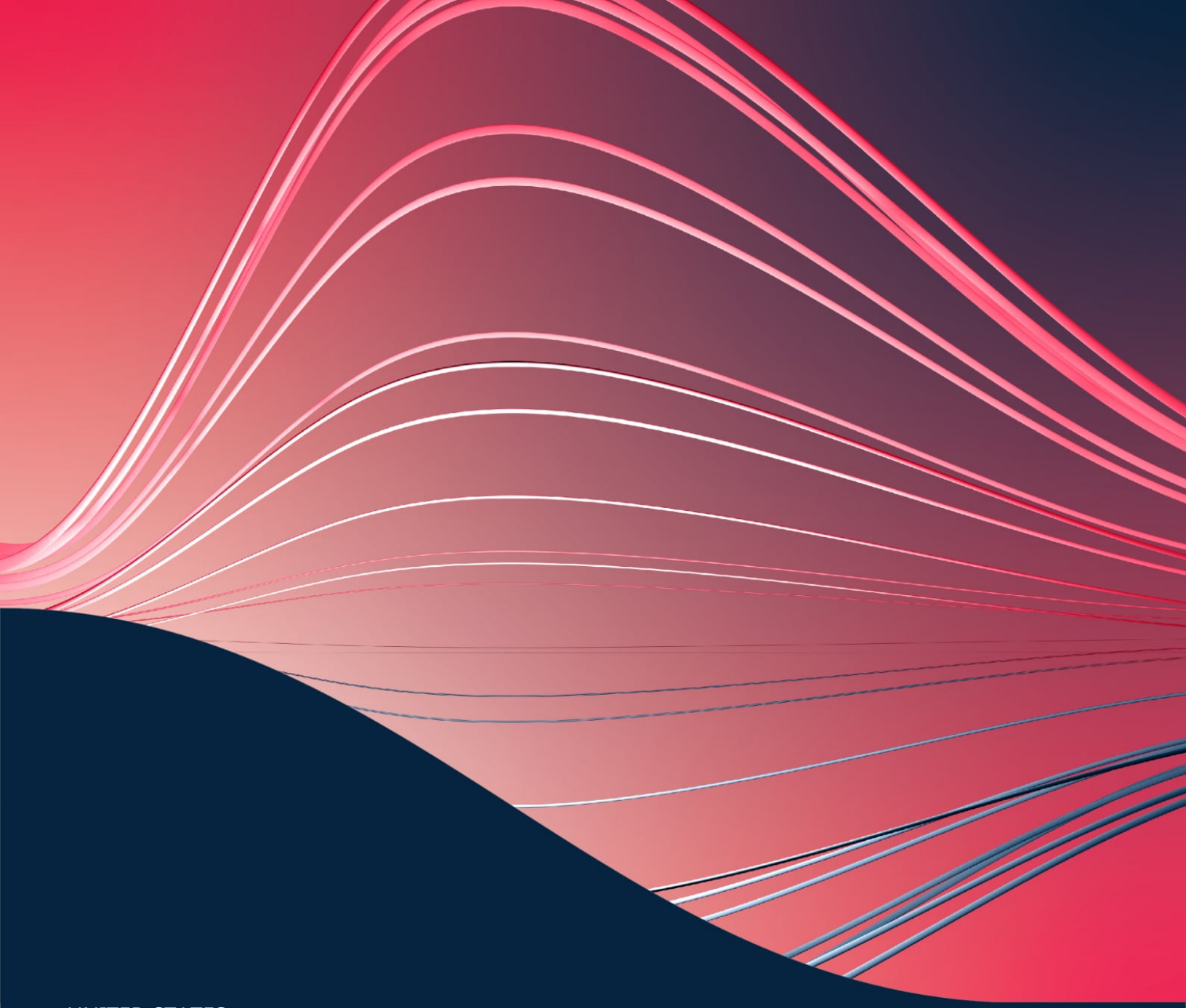


UNITED STATES

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

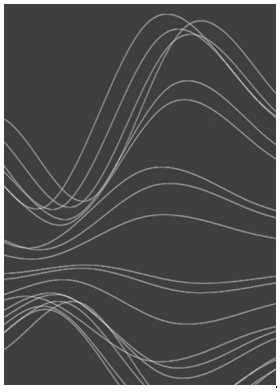
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
ewa.kurowska-tober@dlapiper.com
Full bio

John Magee
Partner
john.magee@dlapiper.com
Full bio

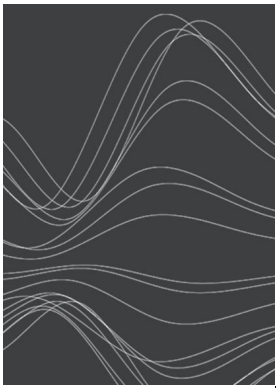
Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

James Clark
Partner
james.clark@dlapiper.com
Full bio

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

United States

LAST MODIFIED 6 FEBRUARY 2025

Data protection laws

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 at the state (and local) level. In recent years, beginning with California in 2018, states have begun to introduce and enact their own comprehensive privacy laws. Although bipartisan draft bills (e.g., the American Privacy Rights Act of 2024) have been introduced since then , changes in the political climate, industry influence, and the increasing complexity of privacy concerns have stifled efforts of passing an omnibus law. Thus, a comprehensive privacy law on the federal level is not expected to pass any time soon.

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 online privacy, telemarketing, email marketing, biometrics, and communications privacy laws.

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

For example, California alone has more than 25 state privacy and data security laws, including the comprehensive CCPA, which provides definitions and broad individual rights and imposes requirements and restrictions on the collection, use, disclosure, and processing of personal information of CA residents. The CCPA is unique among the existing state comprehensive privacy laws in that, it applies not only to personal

information related to consumers but also in the HR and B2B context. Enforcement of the updated CCPA regulations, which were finalized March 29, 2023, commenced on March 29, 2024, by the newly established California Privacy Protection Agency, referred to as the 'CPPA' or 'Agency.' On November 8, 2024, the Agency Board voted to commence supplementary CCPA rulemaking on certain additional regulatory subjects: CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies. Specifically, the proposed regulations seek to (1) update existing CCPA regulations; (2) implement requirements for certain businesses to conduct privacy risk assessments and complete annual cybersecurity audits; (3) implement the right to access and opt-out of being subject to ADMT; and (4) clarify when insurance companies must comply with the CCPA. The public comment period for these proposed regulations closes on February 19, 2025.

The CPPA also enforces the "Delete Act," effective January 1, 2024, which imposes deletion obligations on data brokers, thereby allowing consumers to more easily delete their personal information held by data brokers in California. Under the Delete Act, the CPPA must establish an accessible deletion mechanism by January 1, 2026. This mechanism is intended to allow consumers to make a single verifiable deletion request to have their data deleted by data brokers and their associated service providers or contractors.

In August 2022, the California legislature passed the California Age-Appropriate Design Code (CAADC), which was slated to take effect July 1, 2024, and would apply to companies that meet the definition of "business" under the CCPA and that provide online services that are likely to be accessed by individuals under 18 years of age. However, on September 18, 2023, a California District Court issued an injunction blocking the law from coming into effect on First Amendment grounds. Following an appeal to the Ninth Circuit by the California Attorney General's office, the fate of the law is currently uncertain. More information on the California Age-Appropriate Design Code is available online.

Similarly, Maryland has enacted the "Kids Code" and Connecticut amended its Consumer Data Protection Act to include similar protections for children's personal information. Moreover, in January 2025, the Federal Trade Commission (FTC) finalized significant changes to the federal Children's Online Privacy Protection Act (COPPA). While the FTC periodically reviews the COPPA rule, these rule changes are the first amendment to COPPA since 2013. According to the FTC, the final amended rule reflects technological advancements since COPPA was last amended and is intended to enhance online safety for children. More information on the amended rule is available online. The combined efforts of federal and state regulators are intended to pave the way for a safer digital landscape and ensure that children's privacy is prioritized in an increasingly connected world.

Beyond California's CCPA, additional comprehensive state privacy laws have also taken effect, including the

- Colorado Privacy Act, Connecticut Data Privacy Act (including amendments regulating consumer health data, children's data, and social media platforms),
- Delaware Personal Data Privacy Act,
- Florida Data Privacy and Security Act,

- Iowa Consumer Data Protection Act,
- Montana Consumer Data Privacy Act,
- Nebraska Data Privacy Act,
- New Hampshire Consumer Expectation of Privacy Act,
- New Jersey Personal Data Privacy Act,
- Oregon Consumer Privacy Act,
- Texas Data Privacy and Security Act,
- Utah Consumer Privacy Act, and
- Virginia Consumer Data Protection Act.

While not identical, the these comprehensive state privacy laws are, with the exception of the CCPA, substantially similar to each other in most respects, but may differ in certain regards, for example, scope, privacy notice disclosures, privacy rights, and certain key definitions. These state laws are also generally inapplicable to personal information collected about, and processed in the context of, employee and business relationships. While the CCPA has some practical similarities with these state laws, it adopts more granular definitions, requirements, and restrictions that vary considerably from these laws, and, notably, also applies to personal information collected from California residents in employment and B2B contexts.

There have also been significant developments in the health data space, beginning in 2023 with Washington passing the landmark My Health My Data Act (MHMD). The law ostensibly applies only to consumer health data, but its exceptionally broad definitions and scope combined with its private right of action may mean its enforcement touches on data many companies may not typically consider "health" data. More information on the MHMD Act is available online. Since MHMD, other states have followed suit—Nevada passed the Nevada Consumer Health Data Privacy Law through senate bill 370, effective March 31, 2024, and Connecticut amended the Consumer Data Privacy Act to include similar provisions for protecting consumer health data, effective October 1, 2023.

Finally, the pace of state privacy legislation has continued to accelerate overall, with the following states also passing their own comprehensive privacy laws or variations thereof, and even more states introducing similar legislation:

- Tennessee (effective July 1, 2025)
- Minnesota (effective July 21, 2025)
- Maryland (effective November 1, 2025)
- Indiana (effective January 1, 2026)
- Kentucky (effective January 1, 2026)
- Rhode Island (effective January 1, 2026)

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).

Key Areas of Privacy Class Action

Privacy class actions continue to be a significant risk area in the United States, including in the context of biometric privacy (under the Illinois Biometric Privacy Act), text messaging (under the federal Telephone Consumer Privacy Act) and call recording, wiretapping and related claims under the California Invasion of Privacy Act, the Video Privacy Protection Act (VPPA) and other state laws. Online monitoring and targeting activities—including via cookies, pixels, chat bots, and so-called "session replay" tools—are an area of particular focus in the eyes of both regulators and plaintiff 's attorneys. Under the CCPA, data breaches due to inadequate security measures, allow for a private right of action. The highlight the evolving landscape of privacy litigation, emphasizing the need for businesses to comply with stringent data protection regulations to avoid legal repercussions.

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, 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. Excluded from the definition are deidentified information and information lawfully made publicly available through various means, such as through government records or by the consumer.

Under the law, 'consumer' is broadly defined as any resident of California.

Other State Comprehensive Privacy Laws

Under the other eighteen comprehensive state privacy laws, personal data includes information that is linked or reasonably linkable to an identified or identifiable individual, who is a resident of the particular state acting an individual or household capacity. Deidentified data, personal data made publicly available, and personal data about individuals acting in an employment or B2B context are generally 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 CCPA 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, citizenship or immigration status, 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

Other State Comprehensive Privacy Laws

Under the other comprehensive state privacy laws, the definition of *sensitive data* is a sub-cateogry of peronsal data and largely the same with various states adding or subtracting certain data elements from the above list.

Washington

Washington's MHMD Act introduced a very broad definition of *consumer health data*, which includes: "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."

For the purposes of this definition, physical or mental health status includes, but is not limited to:

- Individual health conditions, treatment, diseases, or diagnosis
- Social, psychological, behavioral, and medical interventions
- Health-related surgeries or procedures
- Use or purchase of prescribed medication
- Bodily functions, vital signs, symptoms, or measurements of the information described in subsection (8)(b)
- Diagnoses or diagnostic testing, treatment, or medication
- Gender-affirming care information
- Reproductive or sexual health information
- Biometric data
- Genetic data
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies

- Data that identifies a consumer seeking health care services
- Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in (b)(i) through (xii) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)

This definition could arguably include any category of personal data (e.g., the inclusion of inference data makes it difficult to exclude any data whatsoever in the health, wellness, and fitness space). In addition, "health care services" includes any service provided to a person to assess, measure, improve, or learn about a person's health.

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 and the California Privacy Protection Agency (the Agency) share authority to enforce the CCPA.

California consumers also have a private right of action under the CCPA for certain data breaches, and the CCPA provides for statutory damages.

Other State Comprehensive Privacy Laws

State Attorneys General in all the other states with comprehensive state privacy laws have authority to enforce their state comprehensive privacy laws. Additionally, in some states such as Colorado, district attorneys can enforce the law.

None of these states currently provide for a private right of action.

Washington

The Washington Attorney General has the authority to enforce the MHMD Act.

Washington residents also have a private right of action under the Act, but unlike the CCPA the MHMD Act does not provide for statutory damages, meaning plaintiffs must prove actual damages to succeed.

Sector-Specific Enforcement

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, certain states currently 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 (however, following amendments to the data broker registration law in late 2023, the data broker registration process and list is being transferred to the Agency). 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.

Oregon

In 2023, Oregon passed a law requiring data brokers register on an annual basis with the Department of Consumer and Business Services before collecting personal data in Oregon. Companies must register if they maintain data that is “categorized or organized for sale or licensing to another person.” The law took effect on January 1, 2024.

Texas

In 2023, Texas passed a law requiring data brokers register with the Secretary of State. The law has a narrower scope than most of the other state data broker registration laws in that it only applies to businesses that (1) in a 12-month period, derive more than 50% of their revenue from the processing or transfer of personal data that the business did not collect directly from individuals, or (2) derive revenue from the processing or transfer of personal data of more than 50,000 individuals whose data the business did not directly collect. The law took effect on September 1, 2023, with first registrations due March 1, 2024.

Vermont

In 2018, Vermont 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, including the recently updated FTC Safeguards Rule (applicable to non-banking financial institutions), require organizations to appoint one or more employees to maintain their information security program.

Collection and 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 individuals 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.

All states with comprehensive privacy laws, other than California, Florida, Iowa, and Utah require a business obtain consent from consumers to collect their sensitive data. California requires businesses to provide individuals a right to limit use of their sensitive data, Iowa requires individuals be provided a notice and opportunity to opt out of sensitive data processing for nonexempt purposes, and Utah requires individuals be provided a notice and right to opt-out of the collection of sensitive data.

The (federal) Children's Online Privacy Protection Act (COPPA) requires verifiable parental consent prior to the collection, use, or disclosure of any personal information from children under 13. As of 2025, COPPA also requires separate, specific opt-in parental consent before companies can use children's data for purposes of targeted advertising or disclose it to third parties. In addition, the CCPA requires 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.). Amendments to the CCPA expanded this concept to include "sharing" of a minor's personal information (meaning the disclosing of personal information for purposes of cross-contextual behavioral advertising).

Further, companies generally need to obtain opt-in consent prior to using, disclosing or otherwise processing personal information in a manner that is materially different than what was disclosed in the privacy policy applicable when the personal information was initially 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, which applies to individual and household data about California residents, businesses must, among other things:

- At or before collection, provide a notice to consumers disclosing the categories of personal information to be collected. the purposes for collecting such information, whether such information will be sold or shared, and how long such information will be retained or the criteria to determine such period.
- 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" and "shared" by the business in the prior 12 months
  - the purposes for which the business collects, uses, sells, and shares 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
- Include a “do-not-sell-or-share my information” link on the business's website and page where consumers can opt-out of the sale and sharing 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 the right 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 the comprehensive US state privacy laws, individuals have various qualified rights to request access to, correction, and deletion of their personal information and to “opt out” of sales, sharing, and the use of their personal information for purposes of targeted advertising or profiling. 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

All states other than California and Utah require 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, a method by which the consumer can submit a complaint to the state's 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 are several 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 regarding the storing of some governmental records and information. However, the HIPAA Privacy Rule requires that covered entities not disclose protected health information outside the US without appropriate safeguards.

Executive Order 14117

Additionally, on February 28, 2024, Executive Order 14117 'Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern' (EO), set forth that '[i]t is the policy of the United States to restrict access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States.' Under the EO, the Attorney General is authorized to determine and identify classes of transactions that 'pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data.' In this context 'sensitive personal data' includes covered personal identifiers (such as SSN, passport and government IDs), personal financial data, personal health data, precise geolocation data, biometric identifiers, and human 'omic data or a combination thereof. However, it is important to note that the EO does not broadly set forth general bulk transfer restrictions, but is focused on regulating specific transfers that could be of concern to national security.

Pursuant to the EO, following its Advance Notice of Proposed Rulemaking (ANPRM) publication in the Federal Register on March 5, 2024, and subsequent Notice of Proposed Rulemaking (NPRM) from October 21, 2024, the Department of Justice (DOJ) issued its Final Rule to implement EO 14117 (Rule) to the EO. The Rule sets forth definitions, countries of concern, in-scope covered persons and defines prohibited, restricted, and transactions exempt under the Rule. In addition the Rule addresses the

relevant processes to obtain licenses to authorize otherwise prohibited or restricted transactions, provides protocols for the designation of covered persons, and sets forth requirements related to advisory opinions, and recordkeeping, reporting, and other audit and due diligence obligations applicable to covered transactions. The Rule will come into effect 90 days from the date of the Rule's publication, with certain requirements (*eg*, due diligence, reporting, and auditing requirements) coming into effect 270 days after publication. The DOJ announced that it intends to publish additional compliance, enforcement, and other practical guidance and clarifications. Such supplemental guidance will be located at www.justice.gov/nsd/data-security.

Final Rule to implement Executive Order 14117

Under the Rule certain highly sensitive transactions are prohibited in their entirety ('prohibited transactions'), while other classes of transactions are restricted but permitted to the extent they comply with predefined security requirements to mitigate the risk of access to certain high-risk 'bulk data' by 'countries of concern' ('restricted transactions'). The Rule prohibits or limits U.S. persons from engaging in prohibited and restricted transfers that pose an unacceptable risk of providing 'countries of concern' or 'covered persons' access to US government-related data or bulk sensitive personal data as such terms are defined under the EO and Rule. Accordingly the Rule:

- classifies:
  - prohibited, restricted, and exempt transactions
  - countries of concern to which the prohibitions and restrictions apply
  - covered persons to which the prohibitions and restrictions apply, and
- identifies and establishes:
  - the processes for licensing and advisory opinions
  - threshold for applicability of the prohibitions and restrictions on covered data transactions involving bulk sensitive personal data
  - recordkeeping, auditing reporting, and other compliance requirements, and
  - enforcement mechanisms including civil penalties

Key Definitions and Classifications under the Rule

Countries of Concern

The Rule identifies six countries as countries of concern:

- China (including Hong Kong and Macau)
- Cuba
- Iran
- North Korea
- Russia, and
- Venezuela

Sensitive Personal Data

Under the Rule the definition of sensitive personal data includes covered personal identifiers (e.g., names linked to device identifiers, Social Security numbers, driver's license, or other government identification numbers), precise geolocation data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof.

Notably, the definition categorically excludes public or nonpublic data that does not relate to an individual, including trade secrets or proprietary information (that meet the relevant definition), data that is, at the time of the transaction, lawfully available to the public from a Federal, State, or local government record (*eg*, court records) or via widely distributed media (*ie*, sources generally available to the public via unrestricted access), personal communications, and information or informational materials, including ordinarily associated metadata or metadata reasonably necessary to enable the transmission or dissemination of such information or informational materials.

Bulk Data

The term 'bulk' refers to any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the prior 12 months, regardless whether through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign or covered person:

- human genomic data collected or maintained on 100+ U.S. persons
- human 'omic data collected or maintained on 1,000+ U.S. persons
- biometric identifiers collected or maintained on 1,000+ U.S. persons
- precise geolocation data collected or maintained on 1,000+ U.S. devices
- personal health data collected or maintained on 10,000+ U.S. persons
- personal financial data collected or maintained on 10,000+ U.S. persons
- certain covered personal identifiers collected or maintained on 100,000+ U.S. persons
- any combination of the above data types that meets the lowest threshold for any category in the dataset

Bulk U.S. Sensitive Personal Data

The term 'bulk U.S. sensitive personal data' means a collection or set of sensitive personal data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds the applicable threshold set forth above.

Covered Data Transaction

A 'covered data transaction' is any transaction that involves any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involves:

- Data brokerage

- A vendor agreement
- An employment agreement, or
- An investment agreement

U.S. persons engaged in data brokerage with foreign persons who are not covered persons must comply with minimum conditions, including putting in place contract terms that prohibit the foreign person from subsequently reselling or providing access to the transferred data to countries of concern or covered persons.

Restricted Transactions

The Rule provides for three categories of 'restricted transactions':

- vendor agreements
- employment agreements, and
- non-passive investment agreements

In contrast to 'prohibited restrictions,' the rule permits 'restricted transactions,' provided that certain security requirements developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA), are met to mitigate the risk of access by any 'countries of concern' or 'covered persons.' Restricted transactions involving access by countries of concern or covered persons to 'bulk U.S. sensitive personal data' or 'U.S. Government-related data' must comply with separate security requirements developed by CISA in coordination with the DOJ. Accordingly, CISA has also published its own proposed security requirements for public comment and will publish final requirements separately through the Federal Register and on its website. As proposed, CISA's security requirements would include the following cybersecurity measures on a data and system level:

- organizational cybersecurity policies and practices
- physical and logical access controls
- data masking and minimization
- encryption, and
- privacy-enhancing techniques and design

Reporting Requirements

Under the Rule, certain U.S. persons must comply with reporting requirements to demonstrate compliance and safeguard national security. These include:

- Annual reports filed by U.S. persons engaged in restricted transactions involving cloud-computing services, if they are 25% or more owned, directly or indirectly, by a country of concern or covered person

- Reports by any U.S. person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction involving data brokerage
- Reports by U.S. persons engaged in a covered data transaction involving data brokerage with a foreign non-covered person if the U.S. person knows or suspects that the foreign counterparty is violating the restrictions on resale and onward transfer to countries of concern or covered persons, and
- Reports by U.S. persons invoking the exemption for certain data transactions that are necessary to obtain or maintain regulatory approval to market a drug, biological product, device, or a combination product in a country of concern

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 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 " SHIELD 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 and Washington's MHMD Act provide a private right of action to individuals for certain breaches of unencrypted personal information or consumer health data, respectively, which increases class action risks posed by data breaches.

There are also several 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 federal Gramm-Leach-Bliley Act and implementing rules and 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 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.' To the extent a device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature if (i) the preprogrammed is unique to each device manufactured, or (ii) the device forces the user to set a unique password upon first use.

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 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. Further, certain states require impacted individuals to be provided with credit monitoring services for specified lengths of time if the breach involved Social Security numbers. Finally, 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, particularly for uncooperative or repeat offenders.

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.

The CCPA 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. Currently, no other comprehensive state privacy laws contain a private right of action.

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' (*e.g.*, 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. 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, under most of the comprehensive state laws, information collected via cookies, online, mobile and targeted ads, and other online tracking are 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. 'Sharing' under the CCPA is defined as sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged. These broad definitions 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.

Universal Opt-Out Signals / Global Privacy Control (GPC)

Amendments to the CCPA, and recent enforcement actions by the California Attorney General, have highlighted the requirement that businesses that process personal information for targeted advertising purposes allow consumers to opt-out of sales and sharing, using an opt-out preferences signal sent by the consumer's browser or a

browser plugin, aso referred to as Global Privacy Control (GPC). Colorado's comprehensive privacy law introduces the same requirement, with an effective date of July 1, 2024.

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.

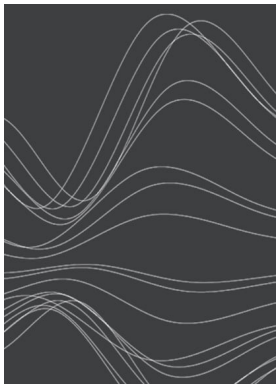
Location Data

Generally, specific notice and consent in needed to collect precise *(e.g.,* mobile device) location information. The CCPA defines precise geolocation information as "any data derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet." Connecticut and Utah law carry similar definitions, albeit with a radius of 1,750 feet.

Data protection lawyers

Kate Lucente
Partner
DLA Piper
kate.lucente@us.dlapiper.com
View bio

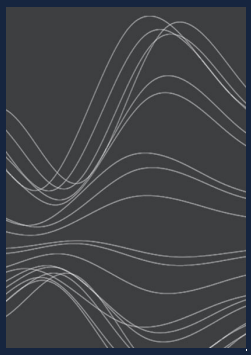
Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
DLA Piper
andrew.serwin@us.dlapiper.com
View bio



Jennifer M. Kashatus
Partner
DLA Piper
jennifer.kashatus@us.dlapiper.com
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com

This publication is for general information only. The information presented is not legal advice, and your use of it does not create a lawyer-client relationship. All legal matters are unique and any prior results described in this publication do not guarantee a similar outcome in future matters. DLA Piper is a global law firm operating through DLA Piper LLP (US) and affiliated entities. For further information, please refer to dlapiper.com. Attorney Advertising. Copyright © 2025 DLA Piper LLP (US). All rights reserved.