PANORAMIC

DATA PROTECTION & PRIVACY

USA

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: November 21, 2025

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

USA

Morgan Lewis & Bockius LLP

Morgan Lewis

Ezra D Church ezra.church@morganlewis.com
Rimsha Syeda rimsha.syeda@morganlewis.com
Heather Egan heather.egan@morganlewis.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The United States (US) does not have a single comprehensive national law. Instead, privacy and data protection have historically been regulated in the US by general consumer protection law at the federal and state levels that broadly prohibit 'unfair or deceptive acts or practices'.

These general consumer protection laws are supplemented by a patchwork of federal and state laws regulating privacy and data security in respect of certain sectors, types of data and types of conduct. In response to the lack of comprehensive legislation at the federal level, since 2018, a growing number of US states have adopted 'comprehensive' privacy laws. These laws typically apply only to covered entities doing business in the state and they contain carveouts and thresholds for triggering application of the law, as explained in more detail below.

At the federal level, key laws regulating privacy include the following.

- The Gramm-Leach-Bliley Act (GLBA) and its implementing rules, which apply to financial institutions and regulate the collection and disclosure of non-public personal information.
- The Health Insurance Portability and Accountability Act (HIPAA) and its implementing rules, which apply to healthcare providers, health insurers and vendors who support them and regulate protected health information.
- The Fair Credit Reporting Act (FCRA) as amended by the Fair and Accurate Credit Transactions Act (FACTA), which primarily regulates the collection, use and dissemination of consumer credit information for decisions about credit, employment, insurance and housing and that establish a framework for preventing identity theft by helping consumers protect their credit information and making sure it is accurate.
- The Children's Online Privacy Protection Act (COPPA), which governs the online collection of personal information from minors under the age of 13.
- The Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records maintained by schools receiving federal funding.
- The Video Privacy Protection Act (VPPA), which regulates the disclosure of video viewing history information.
- The Electronic Communications Privacy Act (ECPA), which regulates wire, oral and electronic communications while those communications are being made, are in transit and when they are stored on computers, through three titles – Title 1 (known as the Wiretap Act), Title II (known as the Stored Communications Act (SCA)) and Title III, which addresses pen register and trap and trace devices.

- The Telephone Consumer Protection Act (TCPA) and similar state laws, which together regulate telemarketing and other commercial calls, text messages and faxes, including placing heightened restrictions on autodialed, prerecorded and AI voice calls.
- The Telemarketing Sales Rule, which requires telemarketers to disclose material information, prohibits misrepresentations, sets quiet hours and provides for a Do-Not-Call registry.
- The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, which regulates commercial email.
- The Cable Communications Policy Act of 1984 (the Cable Act), which grants cable subscribers rights to their personal information, requires cable providers to get consent for collecting and disclosing data and sets limits on what they can share without permission.
- The Privacy Act of 1974, which applies to federal agencies and governs the collection, maintenance and dissemination of records about individuals maintained in government records.
- The Genetic Information Nondiscrimination Act of 2008 (GINA), which is designed to protect individuals from discrimination based on genetic information in health insurance and employment.
- The Federal Information Security Management Act of 2002 (FISMA), which establishes a framework for securing federal information systems.
- The Cybersecurity Information Sharing Act (CISA), which encourages private entities to share cybersecurity threat indicators and defensive measures with federal authorities.

In addition to federal law, many states have enacted their own privacy and data protection laws. California led the effort when it enacted the California Consumer Privacy Act (CCPA) in 2018 (effective January 2020). The CCPA, later amended and expanded by the California Privacy Rights Act (CPRA), effective 1 January 2023, is one of the first significant comprehensive state privacy laws in the US inspired in part by international models like the European General Data Protection Regulation (GDPR). It established consumer rights regarding personal information, broadly defined and imposed corresponding obligations on businesses across industries, rather than only within a single sector. The CCPA's terminology and concepts (such as data subject rights to access or delete personal information and restrictions on 'selling' personal information) borrow from global privacy norms, adapted to the US context.

A growing number of other states have followed California in implementing state privacy laws. As at the time of writing, 19 US states have enacted 'comprehensive' consumer privacy laws:

- California (CCPA as amended by the CPRA);
- Colorado (the Colorado Privacy Act);
- Connecticut (the Connecticut Data Privacy Act);
- Delaware (the Delaware Personal Data Privacy Act);
- Indiana (the Indiana Consumer Data Protection Act);

- Iowa (the Iowa Consumer Data Protection Act);
- Kentucky (the Kentucky Consumer Data Protection Act);
- Maryland (the Maryland Online Data Privacy Act);
- Minnesota (the Minnesota Consumer Data Privacy Act);
- Montana (the Montana Consumer Data Privacy Act);
- Nebraska (the Nebraska Data Privacy Act);
- New Hampshire (the New Hampshire Consumer Data Privacy Act);
- New Jersey (the New Jersey Personal Data Privacy Act);
- Oregon (the Oregon Consumer Privacy Act);
- Rhode Island (the Rhode Island Data Transparency and Privacy Act);
- Tennessee (the Tennessee Information Protection Act);
- Texas (the Texas Data Privacy and Security Act);
- Utah (the Utah Consumer Privacy Act); and
- Virginia (the Virginia Consumer Data Protection Act).

While these laws are generally referred to as 'comprehensive', most exempt small- to medium-sized businesses and contain industry exemptions and other carveouts that, at least to non-Americans, would seem to contradict that label. But this notion of being 'comprehensive' must be viewed through the lens of federal privacy legislation, referenced above, which focuses only on specific sectors, data or business practices.

The states have taken two main approaches to their comprehensive privacy laws. The first is California, which developed its own distinct framework. The second includes most of the other states, which initially modelled their statutes on the draft Washington Privacy Act (first introduced in 2019, but not yet enacted). To this day, California remains an outlier in several key respects: it is the only state that applies to employee and business contact data and the only state with a dedicated privacy regulator, the California Privacy Protection Agency.

Despite these different approaches, there are many commonalities across the US state privacy laws. Typically, they apply to entities that conduct business in the state and meet certain thresholds – for example, processing the personal data of a set number of state residents or meeting revenue criteria. Covered entities/businesses are subject to obligations under these laws that map to common privacy principles, including those that underlie the GDPR, such as notice and transparency requirements, use limitations, data security requirements and vendor management. They also grant residents various rights over their personal information, such as rights to access, delete, correct or opt out of certain processing of personal information.

As additional state privacy laws have taken effect, their definitions, scope and enforcement mechanisms continue to evolve, including through periodic amendment. Recent amendments to the CCPA and the Virginia Consumer Data Protection Act highlight the divergent paths states are taking as legislatures revisit and refine their approaches. For example, the CCPA amendments expanded consumer rights (eg, right to correction and limiting use/disclosure of sensitive personal information), created an independent regulator (the California Privacy Protection Agency) and tightened business obligations like notice-at-collection. In contrast, the Virginia amendments clarified exemptions (eg, for

nonprofits, employee data), fine-tuned definitions and introduced sector-specific carveouts, reflecting a business-friendly balance. This divergence makes compliance harder for companies, since a 'one-size-fits-all' programme may not always be realistic. Businesses must track not just new state laws, but also ongoing amendments that reshape the rules in different directions.

In addition to the states with comprehensive laws, Florida has enacted the Digital Bill of Rights. While the law might appear to be a comprehensive law because it contains many of the principles found in the other state's laws, Florida's Digital Bill of Rights only applies to companies in the online advertising, smart speaker or app store business that are making over US$1 billion in global annual revenue, which carves out most businesses in that state.

Three states – Washington, Nevada and New York – have enacted health information privacy laws and Connecticut expanded its general privacy law to incorporate Washington's approach. Washington was the first to enact its My Health My Data Act (MHMDA), which sought to fill a gap in the law by protecting consumer health data otherwise not covered by HIPAA. The law defines 'consumer health data' so broadly, it could include any data arguably related to health, wellness, nutrition, fitness or related topics, including inferences and some critics have argued that this definition could basically encompass most types of personal information making this the strictest state privacy law in the country. The law covers entities that conduct business in Washington or that target Washington consumers, as well as 'small business' entities. Covered entities must maintain a consumer health data privacy policy on their homepage, obtain opt-in consent before collecting or sharing consumer health data and put in place protections for covered data. The law restricts geofencing around healthcare facilities and also includes private right of action. While Connecticut, Nevada and New York have passed health information laws similar to Washington (although the NY Governor has not yet signed the NY bill into law), none contain a private right of action.

Three more states, Illinois, Texas and Washington, have enacted biometric information privacy laws. While each of these laws contains slightly different requirements for notice, consent, restrictions on sale and disclosure, security, retention and disposal, only Illinois contains a private right of action. The other states laws are enforced by the state AGs. Many other states regulate biometrics indirectly through their comprehensive privacy laws, where biometric data is categorised as sensitive and triggers heightened protections.

Given the challenge of conducting business in the patchwork environment described above, the US Congress has considered various proposals for a federal privacy law, such as the American Privacy Rights Act. Although bipartisan momentum has been building over the past few years, the proposals have stalled as legislators have failed to reach agreement on key points like pre-emption (whether a federal law would supplant the patchwork of state laws) and whether a federal privacy law should include a private right of action – allowing individuals to sue for violation of the law.

Law stated - 31 October 2025

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The US does not have a single, centralised data protection authority. At the federal level, the US Federal Trade Commission (FTC) is the closest analogue to a primary privacy regulator. The FTC uses its broad authority under section 5 of the FTC Act to prevent 'unfair or deceptive acts or practices' to address privacy and data security violations. The FTC can investigate companies for failing to adhere to their own privacy policies or commitments and for engaging in conduct that unfairly puts consumers' personal information at risk. While the FTC's powers under section 5 traditionally did not include the authority to levy civil fines for first-time violations, the agency can (and frequently does) enter into consent orders, sometimes referred to as consent agreements. A consent order is an administrative settlement: the company does not admit wrongdoing, but agrees to abide by specified obligations (like audits, reporting, consumer redress, deletion of data and more) for a defined period. If a company later violates such an order, the FTC can then seek significant financial penalties.

The FTC also enforces certain privacy laws, including COPPA, under which it can impose fines for violations in the first instance. In recent years, the FTC has been increasingly active in privacy enforcement, investigating issues from big tech companies' data sharing practices to the adequacy of security measures protecting personal information. The Commission also has investigative tools at its disposal, such as the power to issue subpoenas and civil investigative demands to companies to obtain information.

Various other federal authorities have enforcement powers and oversight depending on the law or regulation in question. For example, the US Consumer Financial Protection Bureau (CFPB) (along with federal banking regulators and state financial regulators) enforces privacy and safeguards rules under GLBA for financial institutions; the US Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), enforces HIPAA's Privacy and Security Rules, investigating breaches of protected health information and other violations; the Federal Communications Commission (FCC) enforces customer privacy provisions applicable to telecommunications carriers and addresses unlawful telemarketing practices alongside the FTC. Additionally, agencies like the US Securities and Exchange Commission (SEC) regulate certain cybersecurity practices and disclosures for public companies, such as if a company fails to disclose material cyber incidents or risks. The US Department of Justice (DOJ) can also investigate and prosecute criminal violations of certain privacy-related laws, for example, computer hacking under the Computer Fraud and Abuse Act (CFAA).

At the state level, state Attorneys General (AGs) typically have primary enforcement authority of their state's consumer protection law, as well as their state comprehensive privacy law, if any. State AGs generally can issue subpoenas for information and have reached large monetary settlements over alleged privacy and data security violations. California has established a dedicated enforcement agency for the CCPA, the California Privacy Protection Agency (CPPA). The CPPA is an independent regulator focused exclusively on privacy and can investigate businesses, issue subpoenas, conduct hearings and levy fines of its own for violations of the CCPA.

Agencies may coordinate informally on enforcement. Some federal laws, such as HIPAA and COPPA, also authorise state AGs to enforce violations affecting residents of their respective states. The FTC has often joined state AGs in settlements and businesses are often subject to enforcement under more than one regulatory authority in respect of the same conduct that are alleged to have violated more than one applicable law.

Law stated - 31 October 2025

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The US does not have a single dedicated data protection authority. Federal and state regulators generally are not required by law to cooperate with each other. Each agency or authority operates relatively independently under its own statutory mandate. However, in practice, enforcement authorities often do collaborate voluntarily and for efficiency, especially in high-profile cases such as large-scale data breaches or nationwide privacy violations, where one authority with the closest nexus to the breach may take the lead on enforcement with the others joining in cooperation on investigation and resolution. For example, where a major data breach occurs and has a nationwide impact, state AGs often join a multi-state investigation and settlement. The FTC also coordinates with state AGs when both are investigating the same company's conduct that is alleged to violate privacy or data security requirements. Additionally, federal regulators overseeing specific industries might confer with each other or with state counterparts on overlapping issues – for example, OCR might coordinate with state health departments or insurance regulators in a healthcare breach affecting residents of multiple states.

Law stated - 31 October 2025

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Violations of privacy and data protection laws in the US can result in a range of penalties, predominantly civil (administrative or judicial) and occasionally criminal. The consequences depend on the specific law violated and the egregiousness of the conduct, as different statutes carry different penalty provisions.

While the majority of privacy violations are addressed through civil litigation and regulatory enforcement, wilful or malicious conduct – like hacking, other malicious cyber intrusions or a public company's deliberate concealment of a material data breach – can give rise to criminal liability.

On the civil side, regulatory authorities may impose administrative sanctions or seek court orders against organisations for privacy violations. For example, the FTC can bring enforcement actions against companies for failing to follow their privacy policies or for inadequate data security practices deemed 'unfair' or 'deceptive' under the FTC Act. Such FTC actions can result in consent orders that require the company to implement corrective measures, including establishing comprehensive privacy and information security programmes.

While the FTC historically lacked the power to levy monetary fines for initial privacy violations under section 5, it could fine companies for violating a previously entered FTC order. Moreover, when the FTC enforces statutes that do provide for civil penalties (for example,

COPPA or violations of Do-Not-Call rules under the Telemarketing Sales Rule), it may seek significant fines.

State AGs enforcing state privacy laws can similarly seek civil penalties defined by the respective privacy laws. Many of the new comprehensive state privacy laws set specific fine amounts per violation, with penalties often ranging in the thousands of dollars per violation, subject to caps or discretion of the court. If a company is found to have violated consumers' rights under these state laws, the state AG may file suit and request injunctions, compliance orders and monetary penalties as authorised by the statute. For example, California's CCPA allows civil penalties of up to US$2,500 per violation (or up to US$7,500 per intentional violation or violations involving minors' data), enforced by the state, not including any separate private lawsuits for data breaches.

Criminal penalties are not common in the privacy space, but certain misconduct can lead to criminal enforcement. In the privacy and cybersecurity context, if a company intentionally conceals a breach, lies to investigators or engages in conduct that constitutes wire fraud or obstruction, an enforcement agency might handle the civil and regulatory side, but refer criminal aspects to DOJ or state AG. ECPA, which includes the Wiretap Act and the Stored Communications Act (SCA), criminalises certain intentional interceptions of electronic communications and unauthorised access to stored communications. Similarly, the Computer Fraud and Abuse Act (CFAA) makes it a federal crime to access a computer without authorisation or to exceed authorisation and this law is often applied in hacking cases. Violations of these statutes can result in criminal charges, with penalties ranging from fines to imprisonment, depending on the severity of the underlying conduct, with higher penalties available if the offence was committed for profit, for malicious purposes or caused substantial harm. Many states have parallel state wiretap laws criminalising eavesdropping and unauthorised computer access. In addition, the DOJ has pursued criminal actions against company executives over allegations of concealing data breaches.

HIPAA also authorises criminal prosecution for particularly serious privacy violations in the healthcare sector. The DOJ may prosecute knowing violations of HIPAA's privacy or security rules and convictions may carry fines and even imprisonment with higher penalties if the offence involves intent to sell the data or other aggravating factors.

Law stated - 31 October 2025

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Yes. While there is no single US data protection authority, data owners generally have the right to appeal to the courts against orders of any enforcement authority. The process for appeal depends on the underlying enforcement authority. For example, parties subject to FTC enforcement may seek judicial review of a final agency order under section 5 of the FTC Act by petitioning a US Court of Appeals. Similarly, under HIPAA, covered entities may challenge civil monetary penalties imposed by HHS through administrative appeal procedures, with further review available in federal court.

In general, judicial review of agency action is governed by the Administrative Procedure Act (APA), which allows courts to set aside agency actions that are arbitrary, capricious or

contrary to law. However, because many privacy-related investigations are resolved through settlements or consent orders, judicial review is commonly not pursued.

Law stated - 31 October 2025

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

There is no one single comprehensive data protection law that covers all sectors and types of organisations. Instead, US privacy and data protection law is comprised of a patchwork of laws at the federal and state level that focus on sector (eg, healthcare, financial services, telecommunications), businesses of a certain size (eg, state privacy laws), data viewed to be more sensitive (eg, health information, financial data, biometrics), individuals viewed to be more vulnerable (eg, children, students, workers) and certain business practices (eg, marketing, telemarketing, credit reporting and background checks), for example. This is all backstopped by general consumer protection law at the state and federal levels.

As a result, most sectors and most conduct involving the processing of personal information or other privacy-impacting conduct are covered by some aspect of law and, in many cases overlapping requirements of law. For example, a business that is not engaged in a regulated sector might not be subject to a federal privacy law (aside from the obligation not to engage in deceptive or unfair practices under section 5 of the Federal Trade Commission (FTC) Act), but applicable state laws may still apply. And a healthcare business operating in Washington may be subject to some aspects of the Health Insurance Portability and Accountability Act (HIPAA) as well as the My Health My Data Act (MHMDA).

State comprehensive privacy laws apply across industries but contain many exemptions. Typically, these laws apply to for-profit businesses that meet certain thresholds (eg, they control or process personal data of a specified number of residents in that state or have revenues above a certain benchmark). They often exempt whole categories of organisations or data. Common exemptions apply to government agencies, non-profits, employment or business-to-business data and data already regulated by certain federal laws, such as the Gramm-Leach-Bliley Act (GLBA) or HIPAA. Additionally, activities concerning publicly available information (like data from public records), de-identified data or aggregated data from the definition of 'personal information' and data needed to comply with legal obligations (court disclosures, etc.) are typically exempt.

Law stated - 31 October 2025

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The primary federal law governing interception of communications is the Electronic Communications Privacy Act (ECPA) of 1986, as well as the Wiretap Act, the Stored

Communications Act (SCA) and the Pen Register Act. The Wiretap Act makes it generally illegal to intentionally intercept or record oral, telephone or electronic communications without at least one party's consent, with an exception for law enforcement under court order. This applies, for example, to eavesdropping on phone calls or real-time interception of electronic data streams.

The SCA complements the wiretap aspects of the law by protecting the privacy of communications held in electronic storage, including emails stored on a server, from unauthorised access. In addition to the ECPA, nearly every state has its own wiretapping or eavesdropping law. Some states require the consent of all parties to a communication before it can be recorded ('two-party consent' laws like in California), whereas others mirror the federal rule of one-party consent. Violating these laws can lead to criminal prosecution and private lawsuits. In California, particularly, the California Invasion of Privacy Act (CIPA) has generated extensive private litigation focused on website data collection practices through cookies, pixels and other software. Further, the Computer Fraud and Abuse Act (CFAA) prohibits unauthorised access and exceeding one's authority to access, computers and networks, which can include certain forms of electronic surveillance like installing spyware without permission.

Email marketing is governed by CAN-SPAM, which sets rules for commercial email that require senders to provide an opt-out mechanism, honour opt-out requests, include an accurate subject line and header and not use deceptive content. CAN-SPAM largely pre-empts state laws on email to create a uniform standard, meaning state legislatures cannot impose additional requirements on email beyond what CAN-SPAM requires, with some narrow exceptions. Telemarketing, including text message marketing, is mostly regulated by the Telephone Consumer Protection Act (TCPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act, along with FTC and Federal Communications Commission (FCC) regulations. The TCPA, enforced by the FCC and through litigation, restricts unsolicited marketing calls and text messages, particularly those made using autodialers, prerecorded messages or AI voice. It established the National Do Not Call Registry, giving people a way to opt out of telemarketing calls. Telemarketers are prohibited from calling numbers on that registry (with some exceptions) and the TCPA mandates obtaining prior express consent for certain types of calls (notably, telemarketing robocalls to cell phones require prior express written consent). The FTC's Telemarketing Sales Rule (TSR) also sets rules for telemarketing practices, such as time-of-day 'quiet hour' restrictions and mandatory disclosures and prohibits deceptive telemarketing acts.

In the online context, tracking and surveillance of individual behaviour (through cookies, pixels, etc.) has become a major concern of privacy advocates, but US law addressing it is still developing. While there is not yet a federal law like the EU's ePrivacy Directive or cookie regulations, the California Consumer Privacy Act (CCPA), along with newer state privacy laws, including in Virginia, Colorado, Connecticut and Utah, give consumers the right to opt out of the 'sale' or sharing of personal information for cross-context behavioural or targeted advertising, which has been interpreted to cover some forms of online data sharing for targeted advertising. In addition, California, Colorado, Connecticut, Delaware, Montana, Oregon, Texas and New Jersey also require businesses to honour a universal opt-out signal that lets consumers globally signal their preference not to be tracked or have their data sold. As referenced above, there has been significant private litigation related to these practices under state wiretapping laws, such as CIPA.

Law stated - 31 October 2025

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

Some states have laws addressing privacy in specific contexts; for example, California has CalECPA (requiring law enforcement to get a warrant for accessing electronic communications content) and others have laws on school records and genetic data privacy. Furthermore, privacy law is continually evolving to address artificial intelligence (AI) and automated decision-making. While no comprehensive national AI law exists yet, existing state privacy laws, including the Colorado AI Act and the Minnesota Privacy Act, include provisions on profiling and automated decisions requiring some form of transparency or the right to opt out of purely automated processing that produces legal or similarly significant effects on a consumer.

All 50 US states plus DC and Puerto Rico have laws requiring notification to affected individuals in the event of a 'breach of security' involving their 'personal information'. Each state defines its terms slightly differently, but these laws generally consider 'personal information' to include an individual's name (first name or initial and last name) when combined with another data element such as SSN, driver's licence or state ID number or financial account or credit or debit card number, which could lead to an increased risk of identity theft or financial fraud. Some states have expanded their definitions of personal information to encompass additional elements, such as medical information, health insurance policy numbers, biometric data and online account credentials. The term 'breach of security' generally means unauthorised acquisition of personal information and in a handful of states it also includes unauthorised access to personal information regardless of whether it was acquired.

Where notice is required to be made to an individual, these breach notification laws typically prescribe content for the notice, the timing of the notice, whether credit monitoring is required and whether notice is required to the regulator or other state agency at the time notice is provided to the individual.

In many of these states, in addition to requiring notice of a breach when it occurs, state law also requires that covered persons and businesses implement reasonable administrative, physical and technical safeguards designed to protect personal information. These laws are known as state data security laws and an example of a comprehensive law is Massachusetts, which requires a written information security programme (WISP), specifies the minimum required components of that programme and requires appointment of a data security coordinator.

Law stated - 31 October 2025

PI formats

What categories and types of PI are covered by the law?

There is no single uniform definition of 'personal information' or 'personal data' in the US because the scope of what data is covered by the law varies depending on the law or regulation in question. In general, however, the core concept revolves around information

that can identify or be linked to a specific individual, such as name and address. Some state laws, such as the breach notification laws and state data security laws, define personal information to mean information that could lead to identity theft of financial fraud if compromised, such as individual's name (first name or initial and last name) in combination with another data element such as SSN, driver's licence or state ID number or financial account or credit or debit card number. Some states have expanded their definitions of personal information to encompass additional elements, such as medical information, health insurance policy numbers, biometric data and online account credentials (email address or username together with password or security question answers).

Additional definitions under federal law include 'non-public personal information' under the GLBA; 'protected health information' (PHI) under HIPAA, personal information of children under 13 as defined in the Children's Online Privacy Protection Act (COPPA); and consumer credit and other consumer reporting information, as defined in the Fair Credit Reporting Act (FCRA) and state law equivalents.

The newer comprehensive state privacy laws use more expansive definitions of personal information or personal data, aligned with the European approach. For instance, the CCPA defines 'personal information' broadly as any information that 'identifies, relates to, describes, is reasonably capable of being associated with or could be reasonably linked (directly or indirectly) with a particular consumer or household'. This definition encompasses not just basic identifiers (like name, contact details, government IDs) but also things like purchasing habits, internet browsing history, geolocation data, audio or visual data (eg, photos, recordings), profiles and inferences drawn from other data to create a profile about preferences or behaviour, etc. Under such laws, almost anything from IP addresses to device identifiers to traditional personal identifiers, if linkable to a person, is considered personal data and protected under the law.

Many laws, including most of the new state privacy laws, prescribe a subset of 'sensitive' personal information that require extra protection (more detail on these below). Sensitive personal information definitions may vary depending on the statute, but typically include data like SSN, driver's licence or passport numbers, account credentials, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric information for identification, health data and information about sex life or sexual orientation. Under California's CCPA as amended by the California Privacy Rights Act (CPRA), consumers have a right to limit certain uses of 'sensitive personal information' (eg, limit its use to that which is necessary to perform the services or provide the goods).

Law stated - 31 October 2025

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Unlike the EU's GDPR, which explicitly asserts some extraterritorial jurisdiction (reaching companies outside the EU that target EU residents), US laws do not usually have such clear provisions extending their reach outside of the United States. The crux of US jurisdiction is generally the concept of personal jurisdiction in US courts. Jurisdiction may be case-specific.

State privacy statutes frequently articulate their scope of applicability in terms designed to capture entities well beyond the state's borders, including businesses located in other states or even abroad, so long as they engage with the state's residents. For instance, the CCPA, as amended by the CPRA, applies to any for-profit entity that 'does business in California' and meets specified statutory thresholds, irrespective of the entity's physical location. The statute does not limit 'doing business' to maintaining a physical presence; it may extend to online companies with no offices in California but that offer goods or services to California consumers. Ultimately, however, enforcement presupposes that the entity is subject to the jurisdiction of US authorities, a determination that will be highly fact-dependent.

Law stated - 31 October 2025

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Not all processing of personal information is automatically covered under US privacy law. Most state comprehensive privacy laws apply only where certain threshold conditions are met, such as when a business processes personal information of a defined minimum number of residents (eg, 100,000 consumers) or derives a certain percentage of its revenue from selling personal information. These laws also typically exclude certain data types (eg, publicly available information or de-identified data) and specific entities (eg, government agencies, non-profits or entities regulated by specific federal laws).

The US state comprehensive privacy laws distinguish between businesses/controllers on the one hand and vendors/service providers/processors on the other. In fact, some of the more recently enacted comprehensive state privacy laws explicitly adopt the European terms of controller and processor. Under these laws, a 'controller' is defined as the person or entity that, alone or jointly with others, determines the purpose and means of processing personal data. A 'processor' is an entity that processes personal data on behalf of a controller. Controllers must provide privacy notices to consumers, honour and respond to consumer rights, obtain consent for certain types of processing (like processing sensitive data, in most states) and conduct data protection assessments for high-risk processing. Processors, on the other hand, are required to follow the instructions of the controller and assist the controller in meeting its obligations. The laws typically require that a controller and processor enter into a contract that sets out the scope of processing and includes certain contractual requirements. Key contractual terms required include confidentiality, data security, deletion/return of data after the service is done, engaging sub processors only with consent and more.

California is unique in that the CCPA introduced the term 'business' (meaning the organisation that determines the purposes and means of processing consumers' personal information) and distinguishes the business from 'service provider' or 'contractor' (entities that process personal information on behalf of the business pursuant to a contract, akin to processors). Under CCPA, businesses have the primary responsibility for complying with consumer requests (like access or deletion), for disclosing practices and for ensuring data is handled properly. Service providers are contractually bound to use personal information only for the purposes specified by the business and to assist the business in fulfilling its

obligations (for example, by helping with responding to deletion requests or by not 'selling' the data). Regardless, service providers also have direct obligations and must not use the data they receive from a business for any separate 'commercial' purpose, outside the service they provide.

Under state data breach notification laws, the entity that owns or licences personal information – essentially the data controller – typically has the responsibility to notify affected individuals if they experience a data breach, while the service provider (the data 'processor') that experiences a data breach typically has a duty to inform the controller. However, contractual terms between the controller and processor may impact which entity would ultimately be responsible for notification.

HIPAA also designates 'covered entities' versus 'business associates', who are service providers to those entities who handle health data. Business associates under HIPAA must comply with many of the same safeguards and breach notification requirements by law and by mandatory contract, but covered entities have the primary responsibility for patient rights, similarly to a controller's duty.

Law stated - 31 October 2025

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

US privacy law generally does not require all personal information processing to be grounded in specific legal bases in the same structured way as the GDPR. However, most of the US comprehensive state privacy laws do require that certain types of processing require justification, either through consumer consent or through satisfaction of enumerated permissible purposes.

Federal statutes often place conditions for when personal information may be processed and prohibit certain uses or require consumer notice and consent before particular uses occur. For example, the Health Insurance Portability and Accountability Act (HIPAA) permits covered entities to use and disclose protected health information for treatment, payment and healthcare operations without patient authorisation, but requires specific written authorisation for uses beyond those categories, such as for marketing purposes. Similarly, the Gramm-Leach-Bliley Act (GLBA) allows the sharing of consumer financial information among affiliates but restricts disclosure to non-affiliated third parties unless notice and opt-out requirements are met.

The US state comprehensive privacy laws are more explicit in outlining the grounds upon which data may be processed. These laws typically allow businesses and controllers to process personal information if the processing falls within one of a set of permitted legitimate purposes or if the consumer has provided consent. Commonly permitted purposes include providing requested goods or services, security and fraud prevention, compliance with legal obligations and internal operations related to the context of collection.

Some state privacy laws go further than others by requiring opt-in consent for processing sensitive personal information, which includes information like racial or ethnic origin, health information, sexual orientation, biometric or genetic data and precise geolocation, among others. In such states, consent must be obtained through a clear, affirmative act before such data is collected or used. The California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), while not requiring opt-in for all sensitive data processing, allows consumers to limit the use of their sensitive personal information through a 'Limit the Use of My Sensitive Personal Information' mechanism. Consent is also required under these laws for certain high-risk activities, such as processing children's personal information or engaging in targeted advertising, particularly when combined with profiling or automated decision-making.

Law stated - 31 October 2025

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

While the US lacks a uniform federal definition of 'sensitive' personal information, US state privacy laws distinguish between regular personal information and categories of 'sensitive' personal information. As of 2025, states including California (CPRA), Colorado (CPA), Connecticut (CTDPA), Virginia (VCDPA), Oregon (OCPA), Texas (TDPSA), Utah (UCPA), Montana (MTCDPA), Delaware (DPPA), Iowa (IDPA), Minnesota (MPPA), Maryland (MDOPA), New Hampshire (NHPA), New Jersey (NJPA) and Tennessee (TIPA) have recognised categories of sensitive personal information – typically involving health, biometric, precise geolocation, racial or ethnic data, financial account details and similar categories – as deserving of heightened protection.

Most state privacy laws, such as those in California, Colorado or Virginia, require that sensitive personal information be processed under heightened conditions; for example, California's CCPA allows consumers to opt-out of or limit the processing of their sensitive personal information; Colorado's CPA requires businesses to obtain consumers' opt-in to the processing of their sensitive personal information; while others permit processing if it's 'reasonably necessary' for disclosed business purposes. Maryland's MODPA is unique with a higher threshold and does not rely on only consumer consent. Instead, it prohibits the collection, processing or sharing of sensitive data – defined broadly to include race, religion, health status, sexual orientation, biometric data, precise geolocation and children's data – unless it is 'strictly necessary' to deliver a consumer-requested product or service.

Consumer health data, often a subset of sensitive personal information, also receives additional protections under state law. For example, Washington (the My Health My Data Act) and Nevada (the Consumer Health Data Privacy Law) have enacted specific privacy laws that regulate how businesses can collect, use and share consumer health data; Connecticut amended its state privacy law (CTDPA) in 2023 to include heightened restrictions on processing, sharing and selling consumer health data; and New York recently passed similar legislation (Senate Bill S929) to protect consumers from the unauthorised collection and use of health-related data but the New York Governor has not yet signed that bill into law.

In addition, federal statutes also aim to offer heightened protections for certain types of personal data: health data receives heightened privacy and data security protection under HIPPA; 'non-public personal information' maintained by financial institutions is protected by GLBA safeguards; the Fair Credit Reporting Act (FCRA) governs how consumer reporting agencies collect, use and disclose consumer credit information; and the Genetic Information Nondiscrimination Act prohibits certain uses of genetic information, as well as state genetic information privacy laws.

Relatedly, various state non-discrimination laws restrict the use of certain types of personal information when making decisions about individuals, particularly in areas like housing, employment or access to credit, if doing so would harm members of a protected group. For example, California's Unruh Civil Rights Act prohibits discrimination in public accommodations and in the sale of goods or services based on a broad range of protected characteristics. Depending on the applicable statute, these can include sex, gender, age, race, religion, ethnicity, citizenship, political affiliation, ideology, physical appearance, family status, sexual orientation, health condition, military or veteran status and source of income.

Law stated - 31 October 2025

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

There is no one comprehensive federal privacy law that universally governs the obligation to provide individuals with notice about collection and processing of their personal information. Instead, privacy notice obligations arise under a patchwork of federal and state privacy laws. The Federal Trade Commission (FTC), which serves as the primary regulator in the privacy context, views failure to disclose material data practices as an unfair business practice and inaccurate or omitted information in privacy notices to be a deceptive practice under section 5 of the FTC Act.

At the state level, California continues to require the most prescriptive obligations for privacy notices. The California Consumer Privacy Act (CCPA) applies to both online and offline personal information collection and mandates that businesses present consumers with a detailed privacy notice at or before the point of collection. This notice must disclose, among other elements, the categories of personal information collected, the sources of the information, the business purposes for collection or disclosure, whether the information is sold or shared with third parties (particularly for targeted advertising) and the duration or criteria used to determine data retention. The notice must also explain consumers' rights under the law, including rights to access, delete, correct and limit the use of sensitive personal data and how to exercise them. Where applicable, businesses must include a clear and accessible link titled 'Do Not Sell or Share My Personal Information,' as well as a separate notice regarding the use of sensitive personal information. The California Privacy Rights Act (CPRA) extended these requirements to human resources data and business-to-business (B2B) personal information after the expiration of former exemptions. As such, employees,

job applicants and independent contractors are expected to receive full privacy notices explaining how their data is processed and for what purposes.

Other state privacy laws impose similarly prescriptive notice obligations. Generally, entities must disclose all categories of personal and sensitive data collected, the purposes for processing each category, with whom the data is being shared and what data subject rights are afforded to consumers. This is usually done through a website privacy policy or when the consumer interacts with the entity (often for the first time). Recently, most of the state privacy laws offer similar data subject rights, with the exception of a few nuances (for example, Colorado's CPA requires disclosure of whether profiling is used to make decisions with legal or similarly significant effects on individuals and Minnesota's MNCDPA affords consumers the right to question the result of profiling). While formatting and accessibility standards vary, there is an emerging expectation that notices must be clear, concise and accessible.

In addition to comprehensive privacy statutes, certain federal privacy laws impose specific notice obligations. For example:

- Under the Children's Online Privacy Protection Act (COPPA), operators of websites or online services directed at children under age 13 or that knowingly collect information from such children, must provide a prominent online privacy notice detailing the types of personal information collected, uses, disclosures and parental rights, including rights to review or delete data.
- The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions provide consumers with an initial and annual privacy notice. This notice must outline the types of non-public personal information collected, how it is shared (particularly with non-affiliated third parties) and the consumer's right to opt out of certain types of disclosures. The Consumer Financial Protection Bureau (CFPB) and other agencies maintain model privacy notice forms that, if used properly, grant safe harbour protection.
- The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA), requires consumer reporting agencies and certain data users to provide specific notices in various contexts, including in adverse action letters, identity theft investigations, affiliate sharing and employment screenings.
- The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to issue a Notice of Privacy Practices (NPP) to patients at the time of the first service encounter or as soon as reasonably practicable thereafter. This notice must describe the entity's legal duties, how PHI is used or disclosed and individuals' rights regarding their PHI, including access, amendment and complaints.
- The California Online Privacy Protection Act (CalOPPA) requires any commercial website or online service that collects personal information from California residents to conspicuously post a privacy policy detailing categories of data collected, third-party sharing practices and the operator's response to 'Do Not Track' signals.

Law stated - 31 October 2025

Exemptions from transparency obligations

When is notice not required?

Although most US privacy laws impose obligations to provide notice when collecting or sharing personal information, there are certain circumstances where this duty may not apply. Most notably, notice is not required when the entity collecting data falls outside the scope of the relevant law; for example, if an entity does not meet the applicability threshold with respect to the number of state residents, revenue or volume of data processing.

Law stated - 31 October 2025

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

US privacy law does not impose a general obligation to ensure that personal information is accurate, current or complete. However, state privacy laws increasingly provide consumers with the right to correct inaccuracies in their personal data. For example, under the CCPA/CPRA, CPA, CTDPA, INCDPA, VCDPA and other laws, consumers may request that a business correct inaccurate personal information maintained about them. While these statutes grant correction rights, they do not yet impose prescriptive accuracy standards or require businesses to independently verify or update personal data unless a consumer initiates a correction request.

In contrast, FCRA imposes strict accuracy standards on consumer reporting agencies and those using consumer reports for employment, credit, insurance or other authorised purposes. Agencies must maintain 'maximum possible accuracy' of information and respond to consumer disputes within prescriptive timelines. Consumers have the right to dispute inaccurate information in their credit reports and agencies must investigate and correct inaccuracies.

Under the HIPAA Security Rule, covered entities must ensure the 'integrity' of electronic protected health information (ePHI), including safeguarding against improper alteration or destruction. Although not framed as accuracy per se, this obligation ensures data remains reliable for its intended use.

Law stated - 31 October 2025

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

As an overarching principle, the Privacy Act of 1974 mandates that federal agencies only collect the minimum amount of personal information necessary to accomplish their purposes. The FTC often includes data minimisation requirements as part of its consent decrees at the enforcement level. HIPAA requires covered entities to adhere to a 'minimum necessary' standard when using or disclosing protected health information. Other laws, such as FCRA or the GLBA, emphasise proper use and security rather than explicitly limiting collection practices.

State comprehensive privacy laws do include express data minimisation requirements. Importantly, the trend in state laws is toward tying collection to specific, articulated purposes.

For example, California mandates that businesses collect personal information only to the extent that it is reasonably necessary and proportionate to achieve the purposes disclosed in the notice provided to consumers. Similarly, Virginia's VCDPA, as well as laws in Colorado, Connecticut, Oregon and others, require controllers to limit data collection to what is 'adequate, relevant and reasonably necessary' in relation to the purposes for which the data is processed. These laws also prohibit collection and use of personal data for secondary purposes unless those purposes are disclosed and permitted by law or consent is obtained.

Law stated - 31 October 2025

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

US privacy law does not impose a uniform limit on data retention. Instead, obligations related to data retention are scattered across a patchwork of sector-specific federal laws, general state privacy laws and common law considerations. Where restrictions do apply, they are typically framed around principles of reasonableness, necessity or purpose alignment rather than fixed duration limits.

At the federal level, certain laws impose specific retention requirements based on the type of data and the entity's role. For example, HIPAA requires covered entities to retain specific documentation for six years from the date of creation or the date it was last in effect, whichever is later. Financial institutions may be subject to retention rules under laws such as the Bank Secrecy Act or the GLBA. Employers are subject to retention rules for employment-related records under the Equal Employment Opportunity Commission (EEOC) and Fair Labor Standards Act (FLSA), which include time frames for preserving payroll records and personnel files.

These obligations are typically minimum retention periods rather than maximums. Conversely, there is often an expectation of data deletion or minimisation once data is no longer needed for the purpose for which it was collected. For example, California's CCPA/CPRA mandates that businesses inform consumers, at or before the point of collection, of the length of time they intend to retain each category of personal information – or, if that is not feasible, the criteria used to determine the retention period. Additionally, businesses must not retain personal information 'longer than is reasonably necessary' for the disclosed purposes. BIPA, for example, requires destruction of biometric data either when the initial purpose for collection is satisfied, within three years of the individual's last interaction with the entity or within 30 days of a deletion request. Other state privacy laws similarly require controllers to limit retention to what is reasonably necessary and proportionate to the purposes for which the personal data is processed.

Law stated - 31 October 2025

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes, the concept of purpose limitation, that personal information collected for one reason should not be repurposed for a secondary or unrelated purpose, has become a core principle in US data privacy regulation, particularly through the newer state privacy laws.

Under such state privacy laws, businesses must disclose the specific purposes for which personal information is collected or processed at or before the point of collection. They must limit use of the data to those purposes unless a legal exception applies or the consumer provides affirmative consent for the new use. The laws also prohibit processing personal information in a way that is 'not reasonably necessary or compatible with' the disclosed purposes unless the consumer is notified and, in some cases, consents to the additional processing. This has particular implications for practices like targeted advertising, data monetisation and automated decision-making, which are often treated as separate purposes that require separate justification or opt-out mechanisms.

At the federal level, purpose limitation is more context dependent. HIPAA, for example, restricts use of protected health information to treatment, payment and healthcare operations unless patient authorisation is obtained. Similarly, the GLBA limits financial institutions from using consumer data beyond the original disclosed purposes without affording opt-out rights.

Law stated - 31 October 2025

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

US privacy law does not currently impose broad, uniform restrictions on automated decision-making or profiling at the federal level. However, several state privacy laws have begun to introduce specific rights and limitations regarding decisions made solely by automated means.

The CPRA grants the California Privacy Protection Agency (CPPA) the authority to issue regulations governing the use of personal information in automated decision-making contexts, including profiling. As of mid-2025, the CPPA has proposed draft rules requiring businesses to provide consumers with pre-use notices, opt-out rights and, in certain high-risk scenarios, opportunities to request meaningful human review. These rules apply to decisions that produce legal or similarly significant effects, such as those relating to employment, credit, insurance, housing or access to essential services. While finalisation of these rules has been delayed, enforcement could begin as early as 2026, positioning California as a frontrunner in regulating algorithmic processing of personal information.

Several other state privacy laws, including those in Colorado, Connecticut, Delaware, Oregon and Virginia, provide consumers with explicit rights to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects. These statutes define 'profiling' as any automated processing of personal data to evaluate, analyse or predict personal aspects related to an individual's economic situation, health, preferences, interests,

behaviour, location or movements. Entities subject to these laws are required to disclose the existence of such profiling and must enable individuals to opt out. Minnesota's MNCDPA takes this a step further and affords consumers the right to question the results of profiling. In some jurisdictions, additional duties apply, such as conducting data protection assessments before engaging in high-risk automated processing.

At the federal level, there is currently no general prohibition or consumer right to opt out of profiling or automated decision-making. However, certain federal laws indirectly address the issue. FCRA, for example, requires notice and allows individuals to dispute adverse decisions made based on consumer reports, including automated credit decisions. Likewise, employment and housing discrimination laws may limit the use of algorithms that result in disparate impact, particularly when using protected characteristics as inputs. Federal regulators, including the FTC, have expressed concern about the use of algorithms in ways that may be discriminatory, opaque or deceptive. The FTC has indicated that biased or unexplainable algorithmic decisions may violate section 5 of the FTC Act if they are unfair or deceptive to consumers, particularly if transparency is lacking or explanations are misleading.

Law stated - 31 October 2025

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

US privacy and data protection law imposes a combination of statutory, regulatory and common law security obligations on organisations that handle or process personal information. These obligations vary by sector, data type and jurisdiction but generally require covered entities to implement 'reasonable' administrative, technical and physical safeguards to protect data from unauthorised access, use or disclosure. There is no single uniform standard, but several statutes and enforcement agencies have shaped the key expectation that data security programmes be risk-based, proportionate and documented.

At the federal level, key sector-specific laws impose security requirements:

- The Health Insurance Portability and Accountability Act (HIPAA) mandates that covered entities and business associates maintain appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of electronic protected health information (ePHI). The HIPAA Security Rule, which has proposed updates pending by the Department of Health and Human Services (HHS), prescribes implementation specifications, including access controls, audit logging, encryption and workforce training. Covered entities must also conduct periodic security risk assessments and maintain policies and procedures documenting their security posture.
- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to implement comprehensive information security programmes under its Safeguards Rule, recently updated by the Federal Trade Commission (FTC) in2023 to expand requirements. Covered entities must now designate a qualified individual to oversee the programme,

conduct written risk assessments, monitor service providers for compliance, implement multi-factor authentication and conduct annual reporting to boards of directors.

- The FTC, through section 5 of the FTC Act, has long asserted that failure to implement reasonable security measures can constitute an unfair practice. The FTC has developed de facto standards through enforcement actions for what constitutes reasonable data security. These include regular risk assessments, encryption of sensitive data, employee training, secure software development, vulnerability testing and incident response preparedness.
- The Children's Online Privacy Protection Act (COPPA) requires covered entities to 'establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.

In addition to sector-specific requirements, many state laws impose direct or indirect security obligations. Massachusetts Regulation 201 CMR 17.00 mandates a written information security programme (WISP) with technical and administrative safeguards. New York's SHIELD Act similarly requires businesses to adopt safeguards appropriate to the size and complexity of the business, the nature of the data and the risk of harm. Additionally, the NYDFS Cybersecurity Regulation (23 NYCRR Part 500) imposes specific, prescriptive security requirements on covered financial institutions, including banks, insurance companies and virtual currency businesses operating in New York. Entities must implement a risk-based cybersecurity programme, designate a chief information security officer (CISO), conduct periodic risk assessments and maintain audit trails, multi-factor authentication and encryption for non-public information. BIPA, requires reasonable security measures for businesses handling or processing biometric data. These obligations apply both to data controllers and, through contractual obligations, to processors or service providers.

There are also several cybersecurity standards that are industry specific. For example, the NIST Cybersecurity Framework provides voluntary guidance to assist organisations in identifying and managing critical infrastructure cybersecurity risks (and also offers privacy and cybersecurity frameworks across other industries); the Federal Energy Regulatory Commission (FERC), in collaboration with the North American Electric Reliability Corporation (NERC), establishes and enforces cybersecurity standards for the electric grid through the Critical Infrastructure Protection (CIP) standards that aim to protect the reliability and security of the bulk power system against cyber threats.

Law stated - 31 October 2025

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

As of 2025, all 50 states, the District of Columbia, Puerto Rico, Guam and the US Virgin Islands have enacted data breach notification laws that require organisations to notify individuals (and depending on the criteria, regulators and the media) when specific

categories of personal information are accessed or acquired by unauthorised parties. Several federal statutes also impose breach notification requirements in regulated sectors.

While the specifics vary by jurisdiction, most state breach notification laws apply when a business experiences a security incident that results in the unauthorised acquisition (or, in some states, even unauthorised access) of certain defined types of personal information. The definition of 'personal information' for breach purposes typically includes combinations such as name plus SSN, driver's licence number, financial account credentials, etc. State laws typically require notification to affected individuals without unreasonable delay following the discovery of a breach, subject to specific timing thresholds (eg, 30 or 45 days in certain jurisdictions). In some states, notification must also be provided to state regulators, such as the attorney general, particularly where the breach affects a threshold number of residents (often 500 or more). Several states also mandate notification to consumer reporting agencies when the number of affected individuals exceeds a set threshold. Many statutes permit delays in notification if law enforcement determines that notification would impede an investigation. Additionally, notification may not be required where the organization determines, after a documented risk assessment, that there is no reasonable likelihood of harm to the affected individuals – often referred to as a 'risk of harm threshold'. However, some jurisdictions (eg, California) impose notification duties regardless of risk.

Under NYDFS rules, covered entities must notify the Department within 72 hours of determining that a cybersecurity event has occurred that either (1) triggers notice obligations to another regulator or (2) has a reasonable likelihood of materially harming normal operations. This requirement is independent of consumer notification obligations under New York's general breach statute.

At the federal level, sector-specific breach notification obligations also exist. Under HIPAA, covered entities must notify affected individuals within 60 days of discovering a breach of unsecured protected health information. Notifications must also be provided to the US HHS and, in certain cases, to the media. The GLBA, as interpreted by various financial regulators, requires financial institutions to notify affected individuals and sometimes federal authorities after data breaches involving sensitive financial information. The FTC's Safeguards Rule also imposes incident response obligations on non-bank financial institutions. The Federal Communications Commission (FCC) mandates breach notification under its Customer Proprietary Network Information (CPNI) rules for telecommunications carriers. The SEC, following its 2023 cybersecurity rules, now requires certain public companies to file a Form 8-K within four business days of determining that a cybersecurity incident is material. In addition to legal requirements, US regulators, including the FTC and state AGs, have used enforcement actions to penalise companies for failing to provide timely or adequate breach notifications.

Law stated - 31 October 2025

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Accountability for handling personal information is often operationalised through written policies, training, audits, vendor oversight and formal data governance programmes.

Under the California Privacy Rights Act (CPRA), businesses must implement reasonable security procedures and practices appropriate to the nature of the personal information collected. The law also requires businesses to disclose retention periods, respond to consumer rights requests and ensure that third-party contracts include provisions restricting data use. While not framed expressly as 'accountability,' these requirements together reflect the requirement that internal controls must be documented and enforced. NYDFS also reinforces accountability through its cybersecurity regulation, which requires annual certification of compliance by the board or senior officer, ongoing cybersecurity training and board-level oversight of cybersecurity risks. Amendments over time have strengthened these duties by requiring more detailed documentation of risk assessments, incident response planning and board expertise in cybersecurity oversight.

Other state privacy statutes, including those in Virginia, Colorado, Connecticut, Oregon, Delaware and Texas, introduce explicit accountability requirements for data controllers. These include duties to implement and maintain reasonable administrative, technical and physical data security safeguards; enter into binding contracts with processors that delineate roles, responsibilities and permitted uses of data; and maintain documentation sufficient to demonstrate compliance with the statute.

At the federal level, accountability is enforced largely through sector-specific rules and regulatory expectations. For example, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities and business associates to implement documented policies, designate a security official, conduct periodic risk assessments and provide workforce training. The Federal Trade Commission's (FTC) consent orders in enforcement actions typically mandate that companies develop and maintain comprehensive privacy and data security programmes, including written policies and procedures, board-level reporting and third-party audits for 10 to 20 years. Moreover, emerging federal rules, such as those under the SEC's cybersecurity disclosure requirements, require public companies to maintain controls for identifying and managing cybersecurity risks and to disclose their governance approach to incident response. These rules place increased pressure on boards and C-suites to actively oversee data risk management and documentation efforts.

Law stated - 31 October 2025

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There is no single, uniform requirement to appoint a data protection officer (DPO) under US law, but the law increasingly expects companies to designate responsibility for privacy and data protection to senior personnel with appropriate expertise. However, several laws, particularly sector-specific federal laws and state privacy laws, require organisations to designate individuals or roles with specific responsibilities for privacy or security oversight, creating a functional equivalent of the DPO role.

Most of the state comprehensive privacy laws do not require the appointment of a 'Data Protection Officer' by name. However, several of these laws impose duties that effectively necessitate assigning a senior privacy lead. For example, Colorado requires controllers to document their privacy programme and designate individuals responsible for overseeing data governance and risk assessments; and Connecticut, Virginia, Oregon and other states have similar provisions, particularly around risk assessments, third-party oversight and high-risk processing activities. In these jurisdictions, while no specific title is required, the obligations to manage privacy compliance across functions necessitates the need for designated leadership.

At the federal level, sector-specific statutes explicitly require designations. The HIPAA Security Rule mandates that covered entities and business associates appoint a security officer responsible for developing and implementing security policies and procedures. Under the FTC's amended Safeguards Rule, non-bank financial institutions must designate a qualified individual to oversee their information security programme. That person must regularly report to the board of directors or equivalent governing body on the programme's status, risk landscape and compliance metrics. Additionally, in the FTC's consent orders, companies are often required to appoint a person responsible for privacy or security programme administration. These individuals must report internally and externally, document their activities and sometimes undergo training or certification.

Law stated - 31 October 2025

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Although record-keeping obligations under US privacy law vary depending on the regulation, sector and jurisdiction, an increasing number of laws require that organisations maintain internal documentation relating to their processing of personal information.

Most state comprehensive privacy laws impose implicit or explicit documentation obligations. For example, the CPRA and the Colorado Privacy Act (CPA) require businesses to maintain records of consumer requests and their responses for at least 24 months. Additionally, CPRA regulations mandate record-keeping around certain disclosures, data sales/sharing practices, opt-out mechanisms and risk assessment outcomes. Businesses subject to CPRA audits or enforcement must be able to produce evidence of compliance. Several state privacy laws go further by requiring privacy impact assessments for specific high-risk processing activities, such as targeted advertising, profiling with legal or similarly significant effects or processing sensitive data, including in Delaware, Montana, Oregon, Virginia, Texas and more. These assessments must be documented and retained for regulator review upon request. In many cases, businesses must also keep records of third-party processing contracts, consumer opt-outs and internal decisions relating to purpose compatibility and minimisation.

While not all state laws impose detailed record-keeping rules across the board, best practices now call for maintaining a processing inventory or data map, documenting the categories of data collected, the purposes for which it is used and the legal bases or consumer choices enabling such processing.

By contrast, record-keeping is more defined in regulated sectors at the federal level. Under HIPAA, covered entities must retain privacy-related policies, procedures and complaints for at least six years; the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and SEC cybersecurity rules require documentation of security programmes, risk assessments, board reporting and incident response policies; and the Fair Credit Reporting Act (FCRA), Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA) all include documentation duties specific to the regulated data or activity.

Law stated - 31 October 2025

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

US privacy law, particularly at the state level, increasingly requires controllers to conduct data protection assessments (DPAs) for specific high-risk processing activities. While there is no nationwide obligation to conduct general privacy impact assessments, a growing number of states now impose assessment duties.

Under the CPA, Connecticut's CTDPA, Virginia's VCDPA, Oregon's OCPA and others, controllers must conduct documented risk assessments before engaging in the following activities: processing personal data for targeted advertising; selling personal data; engaging in profiling that presents a reasonably foreseeable risk of legal effects or similarly significant impacts; processing sensitive data; or conducting any processing that presents a heightened risk of harm to consumers. These assessments must identify and weigh the benefits of the processing against potential risks to the rights of the consumer, taking into account safeguards that mitigate those risks. The assessments must be made available to regulators upon request but are generally protected as confidential and exempt from public disclosure.

California's CPRA does not use the term 'risk assessment' per se in the statute, but the California Privacy Protection Agency (CPPA) is empowered to issue regulations requiring businesses to conduct 'privacy risk assessments' for processing that presents significant risks to consumers' privacy. Proposed regulations are expected to define these assessments and may mirror those in other states, including requirements for weighing consumer harm, assessing sensitive data use and reviewing algorithmic fairness and discrimination.

Although not framed as privacy assessments, federal regulators have imposed similar expectations. Under HIPAA, covered entities must conduct periodic security risk assessments to evaluate threats to the confidentiality, integrity and availability of electronic protected health information. The FTC, in enforcement actions, has required companies to perform documented assessments of their data handling practices, particularly where unfair or deceptive conduct is alleged. The SEC's cybersecurity disclosure rules, effective from late 2023, require public companies to assess and disclose material cybersecurity risks, including vulnerabilities and mitigations, effectively embedding a form of risk assessment into securities governance.

Law stated - 31 October 2025

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

An increasingly common trend has been the principle of privacy by design, which means that privacy protections should be integrated into products, services and business processes from the outset. The substance of privacy-by-design obligations can be seen in data minimisation, purpose limitation and risk assessment requirements.

Under California's CPRA, businesses must implement practices that ensure personal information is collected, used, retained and shared only as reasonably necessary and proportionate to the purpose for which it was collected. This includes limiting sensitive data processing and respecting user preferences, such as opt-outs from data sales or targeted advertising, through mandatory technical integrations (eg, honouring Global Privacy Control signals). These requirements, especially when combined with the CPPA's anticipated regulations on automated decision-making and risk assessments, effectively impose privacy-by-design obligations at the system architecture level.

System design obligations are also apparent in vendor management and data protection impact assessment requirements, as controllers must assess whether third-party systems they use comply with privacy commitments and do not introduce excessive risk. In regulated sectors, system design is explicitly mandated. The FTC's Safeguards Rule requires non-bank financial institutions to integrate security into system development life cycles and to test applications for security vulnerabilities; the HIPAA Security Rule calls for technical safeguards to be implemented as part of system configuration and design; and the SEC's cybersecurity rules require public companies to describe how board governance and system-level controls mitigate data and operational risk.

Law stated - 31 October 2025

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

US businesses are not required to register their data processing activities with a centralised authority, nor are they generally required to obtain prior authorisation to process personal information.

There are a few narrow exceptions. Under the Health Insurance Portability and Accountability Act (HIPAA), covered entities must register with the US Department of Health and Human Services (HHS) and maintain updated information in the national provider databases. Under various state data breach laws, businesses must notify designated state agencies (eg, state attorneys general or consumer protection bureaus) in the event of a qualifying breach, but this is event-triggered and not a standing registration.

California's Data Broker Registration Law, now replaced and expanded by the Delete Act (effective January 2026), requires businesses that meet the definition of 'data broker' to register with the California Privacy Protection Agency and maintain annual submissions

regarding their data practices. Of note, this requirement does not apply to all controllers – only those engaged in the sale or licence of personal data with which they have no direct relationship. Similarly, Vermont also requires data brokers to register with the state AG and requires registrants to disclose information on consumer opt-outs, security breaches and more.

Law stated - 31 October 2025

Other transparency duties

Are there any other public transparency duties?

In addition to standard notice requirements, entities are subject to broader public transparency obligations through state privacy laws that vary in scope and application. These duties often relate to data disclosures, profiling practices and the ability of consumers to understand or challenge how personal data is processed and shared.

For example, Minnesota and Oregon's privacy laws allow consumers to request a list of third parties with whom their personal data has been shared. Similarly, Delaware and Maryland laws grant consumers a limited transparency right, allowing them to request specific categories of third parties that have received their personal data. Minnesota's law also establishes a right to question the results of profiling, enabling consumers to obtain an explanation of the logic and rationale behind an automated decision, review the data inputs used in that process and pursue corrective action if they believe the outcome is flawed. These rights go further than the opt-out rights commonly found in other state statutes and align more closely with EU-style transparency around automated processing.

Additionally, as states implement regulations concerning automated decision-making and sensitive data processing, businesses may be required to disclose whether such practices are conducted, whether impact assessments are performed and what consumer safeguards are in place. The Colorado Privacy Act, for example, imposes detailed notice obligations related to profiling, targeted advertising and sensitive data processing, while requiring that businesses maintain and disclose (upon request) data protection assessments for high-risk activities.

Law stated - 31 October 2025

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

US privacy law increasingly requires that entities engaging third-party service providers to process personal information contractually require those processors to act only on behalf of and under the instructions of the entity or controller. Under most state privacy laws, including California's CPRA, Colorado's CPA, Connecticut's CTDPA, Virginia's VCDPA and others, controllers must enter into contracts with any service provider or contractor that receives personal information on their behalf. These agreements must include specific terms, such

as limiting use of personal information to services specified in the contract; prohibiting retention, use or disclosure for the processor's own purposes; imposing obligations to assist the controller with consumer rights requests; mandating the deletion or return of personal data upon termination of services; and requiring the same protections to flow down to any sub processors.

California distinguishes between 'service providers', 'contractors', and 'third parties', each with varying obligations and required contract terms. Notably, the California Privacy Protection Agency (CPPA) prohibits third parties from receiving personal information without the proper contractual terms in place with a business. Service provider contracts should include key terms such as identifying the specific business purposes for disclosure of personal information to the service provider; prohibiting the service provider's processing activities in certain ways (eg, cannot sell/share, cannot combined with other personal information it may have); data protection and data security; and more.

Federally, several laws require service provider relationships to be of contractual nature: under the Health Insurance Portability and Accountability Act (HIPAA), covered entities must enter into 'business associate agreements' with any third-party that handles protected health information, including detailed security and privacy terms; the Federal Trade Commission (FTC) Safeguards Rule requires financial institutions to oversee and contractually bind service providers to implement appropriate security practices; and the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to have contracts in place with service providers to safeguard sensitive non-public information.

Law stated - 31 October 2025

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

State privacy laws generally impose specific restrictions on sharing personal information with third parties that do not qualify as processors or service providers. While the precise obligations vary by jurisdiction, most state laws distinguish between internal disclosures (eg, to service providers or contractors under written agreements) and external disclosures to third parties for purposes such as marketing, targeted advertising or resale, which are more closely regulated.

The California Consumer Privacy Act (CCPA) requires businesses to identify whether they 'sell' or 'share' personal information with third parties. 'Sharing' is defined specifically to include disclosures for cross-context behavioural advertising, even if no monetary consideration is involved. If a business sells or shares personal information, it must provide consumers with a clear right to opt out, including a 'Do Not Sell or Share My Personal Information' link on its website. Importantly, even disclosing data to third parties for analytics purposes may be deemed 'sharing' if the recipient does not qualify as a service provider under the statute's contractual requirements. The CPRA also imposes additional restrictions when the personal information being disclosed constitutes sensitive personal information. In such cases, consumers must be informed of the intended disclosures and granted the right to limit certain uses and onward transfers.

Similarly, under the Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), Virginia Consumer Data Protection Act (VCDPA), Indiana (INCDPA), Montana (MCDPA), Tennessee (TIPA), Utah (UCPA), Iowa (ICDPA) and newer laws like Texas (TDPSA), Oregon, Delaware, New Jersey, New Hampshire, Kentucky and Minnesota, controllers must provide consumers with opt-out rights before sharing data with third parties for targeted advertising or the sale of personal data. Many of these laws define 'sale' to include non-monetary exchanges and impose specific transparency and contractual requirements for disclosures that are not necessary for providing a requested product or service.

These laws generally define 'processors' as entities that process personal information on behalf of the controller pursuant to a binding contract with the necessary terms, such as purpose limitations, confidentiality clauses and rights to audit. Disclosures to entities that use the data for their own purposes or do not have a contract will typically be classified as third-party transfers, triggering opt-out rights and additional compliance obligations.

Law stated - 31 October 2025

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Generally, the US does not impose broad restrictions on cross-border data transfers as seen in the EU's GDPR. However, the Department of Justice's (DOJ) Final Rule on the Prohibition of Bulk Sensitive Data Transfers to Foreign Adversaries (the Final Rule) became effective in July 2025, which imposes restrictions on certain US entities that seek to transfer large volumes of sensitive US personal data to foreign countries identified as 'foreign adversaries', such as China, Russia, Iran and North Korea. The rule does not ban all cross-border transfers, but it prohibits specific covered data transactions and mandates due diligence, reporting and contractual safeguards to prevent unauthorised data access or resale to foreign entities. Covered data includes geolocation, biometric, health and financial information, among others and businesses subject to the rule must contractually prohibit foreign entities from using or disclosing the data onwards.

Law stated - 31 October 2025

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Under the DOJ's Final Rule, extra-territorial data may be 'restricted' where it is shared pursuant to a vendor agreement with a foreign-controlled service provider, as subject to the Final Rule and must comply with the Final Rule's requirements for 'restricted transactions.' A vendor agreement is defined as 'any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration' (§ 202.258). US persons conducting such restricted transactions under the Final Rule must establish a data

compliance programme that, at a minimum, addresses procedures for verifying data flows, procedures to verify identity of vendors and additional requirements.

Law stated - 31 October 2025

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

In general, US privacy law does not impose a data localisation requirement. Businesses are not required to store personal information exclusively within the United States and there is no nationwide mandate that a copy of the data be retained domestically. However, the DOJ's Final Rule, while not a localisation mandate, introduces a localisation pressure by prohibiting or restricting the sale or licensing of certain US datasets to entities in foreign adversary jurisdictions. Businesses subject to this rule may conclude that retaining such data in the US (or restricting access from covered countries) is the most risk-averse approach. Similarly, pursuant to national security agreements, undertaken through US export control laws, the US government may impose data localisation requirements to protect US national security.

Law stated - 31 October 2025

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals have the right to access their personal information under nearly all US state comprehensive privacy laws. This right allows individuals to confirm whether a regulated entity is processing their personal information and to request access to that information. The access right typically includes both the categories of personal information collected and processed, as well as the specific pieces of personal information held about the individual.

To exercise this right, individuals must submit a verifiable request through the methods prescribed by the relevant law. This is usually via at least two designated methods, such as an online form and toll-free number. Businesses are generally required to respond to access requests within 45 days, though a 45-day extension is often permitted when reasonably necessary. Some laws allow consumers to designate authorised agents to submit requests on their behalf.

Limitations to the access right vary by jurisdiction but often include exceptions where disclosure would adversely affect the rights or freedoms of others (for example, revealing trade secrets) or where fulfilling the request would conflict with legal privileges, such as attorney–client privilege. Businesses may also deny requests if they cannot verify the identity of the requestor using reasonable procedures.

In California, the right to access includes the ability to obtain both general disclosures about a business's data practices (eg, what categories of data are collected and for what purposes) and specific information that the business has collected about the individual, provided the individual can be verified. California also requires businesses to state whether data has been sold or shared and to whom. Under the California Privacy Rights Act (CPRA), certain employee data is now within scope of access rights as well.

In addition to the above state rights to access, several key federal statutes also grant this right:

- Health Insurance Portability and Accountability Act (HIPAA): patients have rights to access, request amendments, receive accounting of disclosures and obtain explanations of health record usage.
- Fair Credit Reporting Act (FCRA)/Fair and Accurate Credit Transactions Act (FACTA): consumers may review their credit reports, dispute inaccuracies, receive adverse action notices and correct or suppress certain data.
- Children's Online Privacy Protection Act (COPPA): parents may access, review and delete data collected about their children under 13.

Law stated - 31 October 2025

Other rights

Do individuals have other substantive rights?

Yes. Many of the state and federal regimes discussed above also grant individuals additional substantive data rights beyond access. These include:

- Right to delete: individuals can request that businesses delete personal information collected from them, subject to exceptions (eg, legal retention obligations or security purposes).
- Right to correct: individuals may request the correction of inaccurate personal information, particularly where that data is used in decision-making.
- Right to data portability: individuals can request that their personal data be provided to them in a portable and readily usable format.
- Right to opt out of certain processing: most laws grant the right to opt out of the sale of personal information; targeted advertising/cross-context behavioural advertising; and automated decision-making or profiling with legal or similarly significant effects.
- Right to limit the use and disclosure of sensitive personal information: in California, consumers may restrict businesses from using sensitive personal information beyond what is necessary to perform core services or provide requested goods.
- Right to question results of profiling: individuals in Minnesota can challenge decisions made by automated profiling.
- Right to a recipient list: Minnesota, Maryland, Delaware and Oregon give consumers the right to request the specific recipients (not merely categories) of their personal data.
-

Right to non-discrimination for opt-out: nearly all comprehensive state privacy laws prevent businesses from penalising consumers who opt out or exercise other rights.

Law stated - 31 October 2025

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

In the US, whether individuals have a right to action for monetary damages depends on the specific statute that is allegedly violated, although there is no comprehensive federal law that grants this right. Most state privacy laws do not provide individuals with a general right to action for monetary damages for data protection violations, particularly where no actual harm has occurred. However, limited avenues for monetary recovery do exist under select state laws and certain federal statutes. For example, The California Consumer Privacy Act (CCPA) is unique among the state privacy laws such that individuals may bring a private action for statutory damages where a data breach involves certain types of unencrypted or unredacted personal information and results from a business's failure to implement reasonable security procedures. Statutory damages range from US$100 to US$750 per incident per consumer or actual damages, whichever is greater. Importantly, California courts have generally required concrete harm or risk of harm, such as identity theft, to support standing. The Washington My Health My Data Act also provides a private right of action for consumers to seek actual damages and allows courts to authorise treble damages up to a maximum of US$25,000. Illinois' BIPA also allows individuals to sue businesses that may have illegally collected or handle their biometric data. BIPA, the CCPA and the Telephone Consumer Protection Act (TCPA) award statutory damages even in the absence of showing injury.

With respect to federal privacy laws, the FCRA does allow individuals to recover damages for wilful or negligent violations by credit reporting agencies or data furnishers; the TCPA provides a private right of action for violations and statutory damages in the amount of US$500 for each separate violation and up to US$1,500 for each 'wilful' violation for certain recipients of telephone calls, text messages or other applicable communications in violation of the TCPA; and the Video Privacy Protection Act provides a private right of action for certain disclosures of video rental information.

Additionally, recent litigation has shown private plaintiffs assert common law theories of liability in relation to privacy and cybersecurity practices, such as negligence, breach of contract, unjust enrichment and violations of state laws that prohibit 'unfair or deceptive practices'. US courts generally require individuals to demonstrate 'standing' to bring a claim, meaning the individual must allege a concrete injury that is fairly traceable to the defendant's conduct and likely to be redressed by a favourable decision. The threshold for standing is often lower than the threshold for establishing a right to recover damages. For example, courts may find standing where a plaintiff articulates a credible 'risk of harm', even if actual injury has not yet occurred. Nonetheless, this is typically insufficient on its own to establish the injury element of a statutory claim.

Law stated - 31 October 2025

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

In the US, enforcement of privacy and data protection laws is primarily the responsibility of government authorities and regulatory agencies, although limited access to the judicial system is permitted in specific contexts where private rights of action are afforded by statute.

Enforcement of state comprehensive privacy laws is typically assigned to state AGs, who may initiate investigations, issue subpoenas and bring enforcement actions in civil court. These authorities can seek injunctive relief, impose civil penalties and require companies to adopt corrective measures. California has established a dedicated privacy regulator (the California Privacy Protection Agency) with rulemaking and enforcement powers.

With respect to federal enforcement, the Federal Trade Commission (FTC) acts as the chief privacy enforcer through its authority pursuant to section 5 of the FTC Act, targeting unfair or deceptive practices, including those involving personal information. Although the FTC lacks authority to impose civil penalties for first-time violations of section 5, it may seek injunctive relief, restitution and pursue civil fines for consent order breaches.

Other federal agencies, including the HHS OCR (pursuant to HIPAA), the Consumer Financial Protection Bureau (CFPB) (pursuant to the Gramm-Leach-Bliley Act (GLBA), FCRA) and the Department of Education (pursuant to the Family Educational Rights and Privacy Act (FERPA)), exercise oversight in their respective sectors. Complaints may be filed directly with these agencies, but enforcement actions and penalties are pursued administratively, not through private litigation.

Law stated - 31 October 2025

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

There are multiple exemptions and carve-outs that limit the scope of both the federal and state privacy laws. For example, the CCPA and most other state privacy laws, exempt data that is covered by certain federal regulations, such as HIPAA, GLBA, FCRA, the DPPA, FERPA and COPPA, while other states exempt entities subject to these laws altogether. State privacy laws also generally exempt employee and B2B data (except California); publicly available information, typically defined narrowly as information lawfully made available from government records; and de-identified data, provided appropriate safeguards are in place to prevent reidentification.

Law stated - 31 October 2025

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

While the US lacks a comprehensive federal law specifically regulating the use of cookies or tracking technologies, many state privacy laws impose clear obligations when these tools are used to collect personal information, particularly for behavioural advertising or cross-site tracking.

California's California Consumer Privacy Act (CCPA), as well as privacy laws in Colorado (CPA), Connecticut (CTDPA), Virginia (VCDPA), Oregon (OCPA), Texas (TDPSA), Utah (UCPA), Montana (MTCDPA) and Delaware (DPPA), regulate cookie use when it results in the collection, sale or sharing of personal information. These laws generally require that consumers be notified of the use of tracking technologies and be given the right to opt out of the sale or sharing of their data. California, Colorado, Connecticut, Oregon and Texas also require businesses to honour universal opt-out mechanisms, such as the Global Privacy Control (GPC) and impose contractual requirements on third parties receiving cookie-derived data.

Under the California Privacy Rights Act (CPRA) and Colorado Privacy Act (CPA), businesses must provide a 'Do Not Sell or Share My Personal Information' link or alternative opt-out method. If cookies or pixels are used to collect browsing behaviour and share it with third-party AdTech vendors, this often constitutes a 'sale' or 'share' under these statutes, triggering consumer rights and vendor obligations. Increasingly, regulators have focused on deceptive cookie banner implementations – particularly those that pre-select tracking options, fail to disclose third-party involvement or begin tracking before user consent. Recent enforcement actions by state attorneys general in California, Connecticut, Michigan and Texas have also emphasised the seriousness of sharing sensitive information without clear, affirmative user consent in the context of tracking technologies. Federal regulators have also expressed particular interest in this regard, with the Federal Trade Commission (FTC) actively warning businesses about deceptive or unfair practices related to online tracking and cookie usage, particularly in the context of privacy policies and user consent.

The use of cookies and similar tracking technologies has been a hot topic in litigation over the recent years, with plaintiffs bringing lawsuits under ECPA, SCA, CFAA, tort law and state law equivalents, for example, California's Invasion of Privacy Act (CIPA), alleging that companies used keystroke and other tracking features on websites and mobile apps in violation of such laws. Companies often use their privacy policy disclosures to argue that plaintiffs were on notice of this activity. Some states have ruled in favour of companies, such as Massachusetts' Supreme Judicial Court holding that using third-party website technologies (including Google Analytics and Meta Pixel) does not violate the Massachusetts Wiretap Act. In other states, including California, there are still conflicting opinions in the courts.

Law stated - 31 October 2025

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Electronic marketing is primarily governed at the federal level by the CAN-SPAM Act and the Telephone Consumer Protection Act (TCPA), with increasing overlap from state privacy laws.

The CAN-SPAM Act applies to commercial email messages and mandates accurate sender information, clear identification of advertising content, a physical business address and a functional opt-out mechanism. Businesses must honour opt-out requests within 10 business days and may not charge a fee or require unnecessary information to process an opt-out. The Act does not require prior consent but prohibits misleading or deceptive practices.

The TCPA (and the Telemarketing Sales Rule) regulates marketing through autodialed calls, text messages and prerecorded voice messages. Businesses must obtain prior express written consent for marketing messages delivered through these channels using auto dialers or artificial/prerecorded voices. Violations may result in significant statutory damages and are frequently the basis for class action litigation. Several states have enacted mini-TCPA laws with heightened restrictions. For example, Florida (Florida Telephone Solicitation Act), Oklahoma (Telephone Solicitation Act of 2022) and Maryland (Stop the Spam Calls Act of 2023) impose strict consent requirements and limit the number and timing of marketing communications.

Law stated - 31 October 2025

Targeted advertising

Are there any rules on targeted online advertising?

Most state privacy laws require businesses to provide consumers with a right to opt out of personal data being used for targeted advertising, often enforced through mandatory opt-out links or browser signals. Most states define the term 'targeted advertising' to include ads being displayed to a consumer with a selection based on activities over time and across non-affiliated websites or online applications and based upon prediction of consumer's interests or preferences. The California CCPA/CPRA diverges subtly from the other state privacy laws (and uses the term 'cross-context behavioural advertising') and does not explicitly require the activity to involve tracking behaviour over time or predictive profiling. In contrast, laws such as Virginia, Colorado, Utah and Connecticut clearly require that targeted advertising be based on cross-context tracking and prediction. These states further oblige regulated businesses to provide a clear, accessible opt-out mechanism.

In addition, the FTC requires companies that publicly post privacy policies to ensure the policies are true and accurate to the company's data privacy practices. Therefore, companies that fail to disclose targeted online advertising in their online privacy policies may be subject to enforcement by the FTC.

Industry self-regulatory regimes also recommend certain best practices for targeted online advertising. For example, The Digital Advertising Alliance (DAA) sets self-regulatory principles for targeting online advertising and focuses on transparency and consumer choice and the Network Advertising Institute (NAI) similarly requires participating companies to provide enhanced notice of behavioural advertising practices, honour opt-out preferences and avoid the use of sensitive categories of data without consent.

Law stated - 31 October 2025

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

There are no uniform rules on what constitutes as 'sensitive' personal information, though certain types of data are considered more sensitive. For example, financial data through the Gramm-Leach-Bliley Act (GLBA); health data through Health Insurance Portability and Accountability Act (HIPAA), consumer health privacy laws and general comprehensive state privacy laws, biometric data through biometric and state privacy laws and children's information through Children's Online Privacy Protection Act (COPPA) and state privacy laws, are often subject to heightened protections.

Most state privacy laws, including in California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia, Vermont and Washington, define sensitive data to include information revealing racial or ethnic origin, religious beliefs, mental or physical health conditions or diagnoses, sexual orientation, citizenship or immigration status, genetic or biometric data used to identify an individual, precise geolocation and data collected from a known child. A growing number of states, such as Colorado, Connecticut, Delaware, Indiana, Kentucky, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Vermont and Virginia, require controllers to obtain affirmative opt-in consent prior to processing sensitive personal information. This consent must be specific, informed, freely given and unambiguous and controllers must offer ways to withdraw consent. A smaller subset of states, including Iowa and Utah, allow processing of sensitive personal information if the controller provides clear notice and offers the consumer an opportunity to opt out. These laws generally reflect a more business-friendly posture and do not impose a consent requirement.

In California under the CCPA, businesses are required to provide consumers with a right to limit the use and disclosure of sensitive personal information if the business uses the information for purposes beyond those deemed 'necessary and proportionate' for providing goods or services. This includes use for behavioural advertising, profiling or sharing with third parties. Consumers may exercise this right through a dedicated 'Limit the Use of My Sensitive Personal Information' link.

The Maryland Online Data Privacy Act of 2024 (effective 1 October 2025) is unique and does not rely on consumer consent alone. Instead, it prohibits the collection, processing or sharing of sensitive personal information unless it is 'strictly necessary' to provide or maintain a specific product or service requested by the consumer or required by law.

In addition to consent or limitation rights, most of these laws require controllers to disclose in their privacy notices the categories of sensitive data processed, the purpose of such processing and whether the data is shared or sold. Moreover, several states – including California, Colorado, Connecticut, Indiana, Oregon and Virginia – require data protection impact assessments when processing sensitive data, especially where such processing presents a heightened risk of harm to consumers (eg, for profiling, behavioural advertising or automated decision-making).

Law stated - 31 October 2025

Profiling
Are there any rules regarding individual profiling?

While US federal privacy law does not directly regulate 'profiling' as a distinct category of data processing, certain frameworks have begun to address automated inferences drawn about individuals, particularly where such processing may result in legal or similarly significant effects.

State privacy laws generally define 'profiling' as any form of automated processing to evaluate or predict aspects of a person's behaviour, preferences, economic situation, health or performance, especially when the outcome has a legal or similarly significant impact. These laws generally require consumer opt-out rights of profiling that is used to support decisions producing legal or similarly significant effects, such as those relating to housing, employment or access to essential services. Organisations are typically required to offer opt-outs and may be required to conduct data protection assessments prior to engaging in high-risk processing activities, including profiling that involves sensitive personal information or may heighten the risk of harm to individuals. Although California's CCPA does not yet have finalised regulations on profiling, it authorises the California Privacy Protection Agency (CPPA) to issue rules governing automated decision-making, including profiling. Draft CPPA regulations would require businesses to provide advance notice when profiling is used and to offer consumers opt-out rights in specified contexts.

Law stated - 31 October 2025

Cloud services
Are there any rules or regulator guidance on the use of cloud computing services?

The Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 amended the Stored Communications Act (SCA) to make clear that US law enforcement may compel US-based service providers to produce electronic communications data within their custody or control, regardless of where the data is stored. The CLOUD Act also authorises the US to enter into bilateral agreements with foreign governments to facilitate reciprocal, expedited access to electronic evidence while incorporating privacy and human rights safeguards.

Beyond the CLOUD Act, there is no standalone US federal law governing the use of cloud services, but entities subject to sector-specific laws must ensure that cloud providers meet relevant standards for access control, encryption, data integrity and incident response.

In the healthcare sector, cloud vendors storing or processing protected health information on behalf of covered entities are classified as business associates under HIPAA and must execute business associate agreements that subject them to the same level of data security protection as the covered entity. Similarly, under GLBA's Safeguards Rule, financial institutions must ensure that cloud providers implement effective security measures and comply with third-party oversight requirements.

There are also several standards that outline obligations for specific industries. For example, the Payment Card Industry Data Security Standard (PCI DSS) outlines a set of security controls to protect credit card and cardholder information and cloud service providers must

ensure their infrastructure supports PCI DSS compliance. NIST has also published standards for governing cloud computing, including SP 800-210 (General Access Control Guidance for Cloud Systems) and SP 500-332 (NIST Cloud Federation Reference Architecture.

Additionally, with the Department of Justice's (DOJ) Final Rule on Bulk Sensitive Personal Data now in effect, cloud-based transfers of sensitive personal data to foreign entities may be subject to additional contractual or licensing restrictions, especially where such transfers involve Countries of Concern, as that term is defined by the DOJ's Final Rule.

Law stated - 31 October 2025

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Over the past year, US data protection and cybersecurity law has undergone a significant transformation driven by escalating geopolitical tensions, expanding state privacy legislation and intensified regulatory scrutiny. One of the most consequential developments is the implementation of the Department of Justice's (DOJ) Final Rule on Bulk Sensitive Personal Data, which is now in effect as of April 2025. The Rule imposes sweeping restrictions on the transfer of certain categories of sensitive data – particularly health, biometric, geolocation, genetic and financial data – when such transfers are made in 'bulk' to designated Countries of Concern, including China, Russia, Iran, North Korea, Cuba and Venezuela. The rule introduces both outright prohibitions for certain transactions and a new licensing regime and security programme requirements for others. Multinational companies and data brokers are having to reevaluate cross-border data access, vendor contracts and internal governance of third-country data exposure.

At the same time, state legislatures have accelerated the adoption of comprehensive privacy laws contributing to a patchwork now covering 19 states, plus Florida. Several of these statutes include unique elements, for example, Maryland's data minimisation standard. Notably, the California Consumer Privacy Act (CCPA) and Colorado's Attorney General continue to lead on interpretive rulemaking, especially around profiling, universal opt-out signals and high-risk processing assessments.

There has been a surge in private litigation regarding online data collection practices through cookies, pixels and other technology, with thousands of class actions and arbitrations filed around the US challenging these practices under the federal Electronic Communications Privacy Act (ECPA) and state wiretapping laws. The California Invasions of Privacy Act (CIPA), which includes statutory penalties of up to US$5,000 per violation, has been a particular focus of litigation. This litigation has led to increased adoption of 'cookie banners' and audits of website data collection practices by companies in the US

The outlook for federal privacy legislation remains uncertain. The American Privacy Rights Act, a bipartisan federal bill introduced in 2024, sought to harmonise privacy protections and create a national framework with pre-emption of state laws. However, debates over whether the statute would override stronger state protections, particularly California's, have stalled its

momentum. Until a federal law is enacted, businesses operating in the United States must continue to navigate a complex and shifting compliance environment.

Another major trend is the growing scrutiny of artificial intelligence and automated decision-making. Although the current administration has stated multiple times that it prioritises innovation over regulation, states continue to require statutory opt-outs for profiling decisions that have legal or similarly significant effects, as well as AI-specific laws that include data privacy and protection regulation. For example, Colorado and Utah have comprehensive AI laws (Colorado's AI Act, focusing on high-risk AI systems and Utah's AI Policy Act, focusing on consumer-facing generative AI services and requiring disclosures) and California and New York have specific AI-legislation. Most recently, Texas passed the Responsible Artificial Intelligence Governance Act, which is set to take effect in 2026 and is aimed at prohibiting specific harmful AI practices, particularly those involving governmental use of AI and certain high-risk private sector applications.

There also is an increased awareness on cybersecurity and cybersecurity obligations have deepened, particularly for financial institutions, healthcare entities and publicly traded companies. The SEC's final cybersecurity disclosure rules require registrants to disclose material cyber incidents within four business days and to describe their cybersecurity risk governance at the board and executive level. Concurrently, amendments to the New York Department of Financial Services (NYDFS) cybersecurity regulations now mandate more frequent risk assessments, business continuity planning and independent audits for covered financial institutions. These state and federal initiatives reflect a broader movement toward risk-based cyber governance, with an increasing emphasis on executive accountability.

Law stated - 31 October 2025