

Sensitive Data: Similarities And Differences Across State Privacy Laws

August 2024





Executive Summary

Today, the United States is one of the few large nations without a comprehensive federal privacy law and no generally accepted list of what constitutes sensitive data. In the absence of these, each state legislature is left to decide if, when and how to take up these questions on their own.

While no two state privacy laws are identical in every respect, it is possible to identify certain commonalities that appear to span all or most such laws as well as outlier provisions (or lack of provisions) unique to one or more states. The purpose of this whitepaper is to help illuminate these commonalities and differences.

Privacy Laws are Sectoral, Not Comprehensive

Where privacy laws exist, they address individual sectors. For example federally, The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regulates the use and disclosure of protected health information ("PHI") in healthcare treatment, payment and operations by covered entities and business associates of covered entities. The 2003 HIPAA Security Rule deals specifically with electronic medical records. It specifies administrative, physical, and technical safeguards required for compliance.

Other examples of sectoral law include:

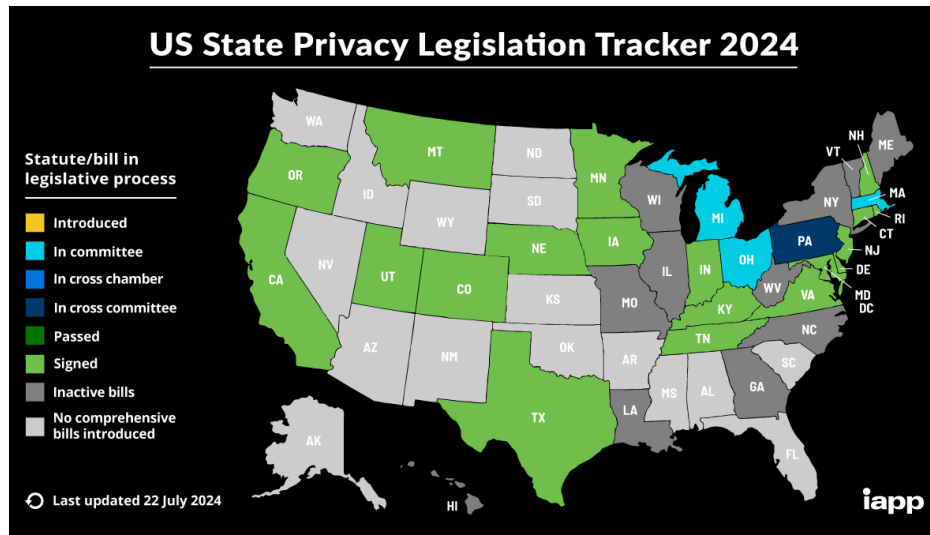
- The Fair Credit Reporting Act ("FCRA")
- The Gramm-Leach-Bliley Act of 2002 ("GLBA")
- The Children's Online Privacy Protection Act ("COPPA")
- The Family Educational Rights and Privacy Act ("FERPA")
- The Video Privacy Protection Act ("VPPA"), The Cable Communications Policy Act of 1984 ("Cable Act")
- The Telephone Consumer Protection Act, ("TCPA")
- The Privacy Act of 1974 ("Privacy Act")
- Section 5 of the Federal Trade Commission Act, (the "FTC Act")

Source: <https://www.privacyworld.blog/summary-of-data-privacy-protection-laws-in-the-united-states/>



The Rise of State Privacy Laws

There has been an explosion in State Privacy Legislation. Privacy Acts went into effect in 2023 in California, Colorado, Connecticut, Utah, and Virginia and are taking effect in 2024 in Montana and Texas. More Privacy Acts will go into effect in 2025 and 2026 in Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, Rhode Island, and Tennessee.



Source: [IAPP](#)

The IAPP Westin Research Center actively tracks the proposed and enacted comprehensive privacy bills from across the U.S. This information is compiled into a map, a detailed chart identifying key provisions in the legislation, and links to enacted state comprehensive privacy laws. These are tracked in the IAPP's [US State Privacy Legislation Tracker](#).



The Rising Concerns About Sensitive Data, and What Sparked It

As the EFF [noted](#) after the Dobbs abortion ruling, the reason for rising concern is that “those seeking, offering, or facilitating abortion access must now assume that any data they provide online or offline could be sought by law enforcement.” Many kinds of sensitive data exist that could be used in “a type of [dragnet surveillance](#) that can compel tech companies to search their records and reveal the identities of all people who have been in a certain location or looked up a particular keyword online. These demands, known as “reverse demands,” “geofence warrants,” or “keyword warrants,” enable local law enforcement in states across the country to request the names and identities of all people whose digital data shows they’ve spent time near a California abortion clinic or searched for information about gender-affirming care online.”

Many kinds of sensitive data exist that could be used in “a type of dragnet surveillance” by law enforcement.



Sensitive Data: Commonalities Among State Privacy Laws

While the privacy laws in California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Montana, Nebraska, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia, Washington, and Nevada all differ in some respects, they share important commonalities.

Definitions Of Sensitive Data

Under many state privacy laws, the following data is considered sensitive.

- **Government identification numbers**, e.g. social security, driver's license, state identification card, or passport number.
- **Financial services data**, e.g. account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
- **Race, religion, and citizenship data**, e.g. racial, ethnic, or national origin, religious beliefs, citizenship or immigration status.
- **Medical and consumer health data**, e.g. medical history, mental or physical health treatment or diagnosis by a healthcare professional, genetic or biometric data.
- **Children's data**, e.g. limited collection of personal information when a child participates in online games and contests, disclosure to parents of any information collected on their children by the website, right to revoke consent and have information deleted.
- **Crime victim data**, e.g. those who are or alleged to be victims of a crime.
- **Sexual orientation data**, e.g. sex life, sexuality. Oregon and Delaware stand alone in adding transgender and nonbinary status to their definitions of sensitive data.
- **Mobility data**, e.g. precise geolocation. The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) classifies precise geolocation data as "sensitive personal information." Virginia and Connecticut both require opt-in consent for the collection and processing of precise geolocation data. The definition of "precise geolocation data" may vary slightly between states. For example, under the CPRA, it's defined as data accurate within a radius of 1,850 feet or less, while other state laws use a radius of 1,750 feet or less.
- **Union status**, e.g. current or past union membership
- **Email and text data** Contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.



Outlier Provisions Among State Privacy Laws

The Washington My Health My Data Act is the first comprehensive privacy-focused law in the United States to protect personal health data that falls outside the Health Insurance Portability and Accountability Act (HIPAA).

Privacy expert James Dempsey [believes](#) a significant portion of health-related data — that which is not in connection with treatment by a healthcare provider (known as a covered entity) — may fall outside of HIPAA's scope and would therefore be defined as sensitive data.

- Its definition of a “consumer” is more broad than other states: it includes Washington residents as well as any individual whose consumer health data is “collected” in Washington.
- Its definition of regulated entities is more broad than other states: it includes any legal entity that conducts business in Washington or produces or provides products or services targeted to consumers in Washington, and that determines the purposes and means of collecting, processing, sharing or selling consumer health data. An entity that only stores data in Washington is not a regulated entity.
- It provides a more broad private right of action than other states.
- Its definition of consumer health data is more broad than other states. “Consumer health data” means personal information that is linked or reasonably linkable to a consumer and that identifies the consumer’s past, present, or future physical or mental health status. This includes prescription medications, bodily functions, measurements, and biometric information. Under this definition, companies that would probably not consider themselves healthcare companies would still be responsible. For example, a concert venue that answers a consumer’s question about wheelchair accessibility, or a company that has made an appointment to install a walk-in shower and grab bars has just collected healthcare information.
- It includes specific protections for reproductive and sexual health information (e.g. gender-affirming care.)
- It specifically includes the right to withdraw consent. What’s more, consent must be obtained prior to the collection or sharing including how the consumer can withdraw consent from future collection or sharing of the consumer’s health data.
- It prohibits geofencing (the use of GPS or RFID technology to trigger a response when a mobile device enters or leaves a virtual geographic boundary.) For example, geofencing around a healthcare facility providing in-person “health care services” as a means to identify, track or target consumers or collect their health data is not allowed. It includes specific protections for reproductive and sexual health information (e.g. gender-affirming care.)



- It specifically includes the right to withdraw consent. What's more, consent must be obtained prior to the collection or sharing including how the consumer can withdraw consent from future collection or sharing of the consumer's health data.
- It prohibits geofencing (the use of GPS or RFID technology to trigger a response when a mobile device enters or leaves a virtual geographic boundary.) For example, geofencing around a healthcare facility providing in-person "health care services" as a means to identify, track or target consumers or collect their health data is not allowed.

A significant portion of health-related data may fall outside of HIPAA's scope and would therefore be defined as sensitive data.

California and Washington each provide consumers with a private right of action. While California only includes this right under very limited conditions (e.g. a data breach), Washington includes a more broad private right of action.

California's protection of child data privacy has been expanded from those under 13 years of age to those under age 18.

Utah passed a law requiring social media companies to provide a parent or guardian "access to the content and interactions of an account held by a Utah resident under the age of 18".

Arkansas passed legislation banning minors under 18 from social media platforms without parental consent.

Utah does not explicitly state a consumer "Right to Correct" inaccurate personal data.



FTC Cases

The FTC took [action](#) against mass data collectors such as Avast, X-Mode, and InMarket for their practices involving the collection and sale of sensitive data, including precise geolocation data. These companies were found to have collected data without proper consumer consent and sold it to third parties, exposing consumers to privacy risks.

The FTC finalized an [order](#) with Global Tel*Link, a telecommunications company, over security failures that led to a breach of sensitive data. The company was found to have inadequate security measures, which resulted in unauthorized access to sensitive personal information, including call records and financial data.

The FTC proposed an [order](#) against Cerebral, a telehealth firm, prohibiting it from using or disclosing sensitive data for advertising purposes. The company was also required to pay \$7 million. This action was taken due to Cerebral's improper handling of sensitive health information, which was used for targeted advertising without proper consent.

The FTC has emphasized the protection of health information through [various cases](#). Key takeaways from these cases include the

importance of obtaining explicit consent for the collection and use of health data, ensuring robust security measures to protect such data, and being transparent with consumers about data practices.

The FTC has committed to enforcing laws against the illegal use and sharing of highly sensitive information, including location and health data. The agency has taken [action](#) against companies that fail to protect this data or use it in ways that violate consumer privacy rights.

In its [2023 Privacy and Data Security Update](#), the FTC highlighted its ongoing efforts to address issues related to sensitive data. The report detailed various enforcement actions and emphasized the need for companies to adopt strong data protection practices to safeguard sensitive information.

The FTC has placed a strong focus on the processing of [sensitive data](#), scrutinizing companies that mishandle such information. The agency's actions include investigating and penalizing businesses that fail to implement [adequate data protection measures](#) or misuse sensitive data for purposes such as targeted advertising without proper consent.



Want to learn how SafeGuard Privacy can save time
and money managing privacy compliance?

Contact us at hello@safeguardprivacy.com
or visit safeguardprivacy.com

