Comparison of US State Privacy Laws

Defining Covered and Sensitive Data

November 2025

Centre for Information Policy Leadership

HUNTON

Table of Contents

Executive Summary

As the patchwork of US state privacy laws continues to expand in the absence of comprehensive federal privacy legislation, the concept of personal information—and the types of personal information categorized as *sensitive*—is a foundational element of privacy compliance. However, the criteria for what qualifies as sensitive—and the legal consequences that follow—are not always aligned across states. As a result, organizations tasked with operationalizing compliance must tailor obligations across a fragmented and sometimes inconsistent legal landscape. Understanding how personal information is conceptualized and categorized determines the applicability of rights, the thresholds for regulatory triggers, and the measures required to protect individuals from harm.

In most jurisdictions, the classification of personal data as *sensitive* triggers stricter consent standards or additional requirements for data protection assessments, regardless of context or the potential of significant harm. For lawmakers seeking to promote innovation, responsible business practices, and individual rights—and for organizations striving to build scalable, effective privacy programs—getting the definitions of covered and sensitive personal data aligned and basing attendant obligations on the risk of harm will ensure greater clarity for consumers and advance a more coherent digital policy.

1. Introduction

Privacy law in the US is a complex matrix of overlapping federal, state, and local laws and regulations. As Congress has yet to pass a comprehensive federal privacy law, more and more state legislatures have adopted laws of their own, aimed at protecting the privacy and security of their residents' personal information.[1] In light of these ongoing state-level developments, organizations' limited resources are stretched to monitor and comply with each legislative nuance.

Given these challenges, CIPL initiated a project to identify alignment and areas of divergence between state laws, and to examine the potential challenges that organizations may face due to these divergences. This paper is the latest in our series, and it should be viewed in the context of our ongoing efforts to support a strong privacy ecosystem in the US, where responsible data practices are promoted, the privacy of individuals is safeguarded, and beneficial uses of data are enabled.

The concept of personal information—and the types of personal information categorized as *sensitive*—has become a foundational element of privacy regulation and compliance. However, the criteria for what qualifies as sensitive—and the legal consequences that follow—are not always aligned across states. As a result, organizations are tasked with operationalizing varying definitions across a fragmented and inconsistent legal landscape.

Understanding how personal information is conceptualized and categorized determines the applicability of rights, the thresholds for regulatory triggers, and the measures required to protect individuals from harm. The varying definitions across states complicate regulatory compliance efforts, risk assessments, and program designs, especially for companies that operate across multiple states, internationally, or those that handle cross-sectoral data.

In most jurisdictions, the classification of personal data as *sensitive* triggers stricter consent standards or additional requirements for data protection assessments, regardless of context or scope of potential harm. Therefore, inconsistent legal trends for defining personal information not only complicate efforts for organizational accountability,[2] but also raise broader questions about whether a categorical approach to data classification is optimal for managing privacy risks in an era of contextual and inferential data processing.

1 **California Consumer Privacy Act of 2018** (CCPA) as amended by the California Privacy Rights Act of 2020 (CCPA), Cal. Civ. Code § 1798.100 et seq.; **Colorado Privacy Act**, Colo. Rev. Stat. § 6-1-1301 et seq., **Connecticut Data Privacy Act**, Conn. Gen. Stat. § 42-515 et seq.; **Delaware Personal Data Privacy Act**, Del. Code. tit. 6, § 12d-101 et seq.; **Florida Digital Bill of Rights**, Fla. Stat. § 501.701 et seq.; **Indiana Consumer Data Protection Act**, Indiana Code § 24-15-1-1 et seq.; **Iowa Consumer Data Protection Act**, Iowa Code § 715D.1 et seq.; **Kentucky Consumer Data Protection Act**, Ky. Rev. Stat. § 367.3611 et seq.(effective Jan. 1, 2026); **Maryland Online Data Privacy Act**, Md. Code, Com. Law § 14-4701 et seq. (effective Oct. 1, 2025); **Minnesota Consumer Data Privacy Act**, Minn. Stat. § 325M.10 et seq.; **Montana Consumer Data Privacy Act**, Mont. Code § 30-14-2801 et seq.; **Nebraska Data Privacy Act**, Neb. Rev. Stat. § 87-1101 et seq.; **New Hampshire Data Privacy Act**, N.H. Rev. Stat. Ann. § 507-H:1 et seq.; **New Jersey Data Protection Act**, N.J. Rev. Stat. § 56:8-166.4 et seq.; **Oregon Consumer Privacy Act**, Or. Rev. Stat. § 646A.570 et seq.; **Rhode Island Data Transparency and Privacy Protection Act**, R.I. Gen. Laws § 6-48.1-1 et seq. (effective Jan. 1, 2026); **Tennessee Information Protection Act**, Tenn. Code Ann. § 47-18-3301 et seq.; **Texas Data Privacy and Security Act**, Tex. Bus. & Com. Code § 541.001 et seq.; **Utah Consumer Privacy Act**, Utah Code § 13-61-101 et seq.; **Virginia Consumer Data Protection Act**, Va. Code § 59.1-575 et seq.; and **Washington My Health My Data Act**, Wash. Rev. Code § 19.373.005 et seq. Florida's law is sometimes considered less than "comprehensive" due to its application to a relatively narrow set of companies, while Washington's law is focused on health but sometimes characterized as "quasi-comprehensive" due to the broad and unique definitions of data covered by the law, as discussed further below. Both are included in this paper given their relevance to the comparative analysis that is its subject.

2 See CIPL resources and papers on organizational accountability at www.informationpolicycentre.com.

For lawmakers aiming to foster innovation, responsible businesses practices, and individual rights—and for organizations working to develop scalable, effective privacy programs—consistent and accurate definitions of covered and sensitive personal data is a public policy priority. Getting rules right for the treatment of sensitive data are also a critical element of a sound enabling environment for development and deployment of AI, as CIPL has discussed elsewhere.[3]

This paper analyzes the scope, applicability, exemptions, and key definitions of covered data under comprehensive state privacy laws.[4] We examine the most common approaches, as well as outliers, with a focus on three topics:

1. The concept of *personal information* (including an analysis of exclusions such as de-identified data and publicly available information)
2. The inclusion of *sensitive data* (or sensitive personal information)
3. Sector-based exemptions

Each topic categorizes particular elements as falling under the *Most Common Approach* or *Other Approaches*. The paper also compares concepts in US state laws to comparable elements of the EU General Data Protection Regulation (GDPR) in light of its importance for many organizations' global compliance programs.[5] We also examine intersecting provisions under key federal laws and regulations.

3 CIPL, Rethinking Sensitive Data in the Age of AI, September 2025.

4 For the purpose of this paper, *comprehensive state privacy laws* means state data privacy laws governing the rights of consumers and imposing obligations on covered entities. These laws generally apply only to non-governmental organizations meeting certain thresholds. They commonly exclude employment-related data (except in California) and provide exemptions, such as for non-profits or certain regulated industries subject to other regulations like the GLBA and HIPAA. *See* footnote 1 for a listing of the specific laws examined.

5 CIPL has written extensively about practical aspects of GDPR implementation, as well as the statute's strengths, weaknesses, and opportunities for reform and improvement going forward. See, for example, CIPL Report, The GDPR's First Six Years: Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement, May 23, 2024.

2. The Concept of Personal Information

At the heart of US state privacy laws lies the concept of personal information. Defining the term *personal information* is foundational in any state privacy law because the law only applies when an entity is processing such information. While broadly understood as data that identifies or relates to an individual, *personal information* is not defined uniformly, reflecting lawmakers' varied interpretations of scope and differing legislative priorities.

Most Common Approach

The most common approach to defining personal information is adapted—albeit with key differences—from the GDPR's definition of the term *personal data*, i.e., "any information relating to an identified or identifiable natural person."[6] Building on this foundation, most states with a comprehensive privacy law[7] define the term with two key characteristics:

Personal Data

a. is information that is linked or reasonably linkable to an identified or identifiable individual; and
b. does not include de-identified[8] or publicly available information.[9]

Under these laws, data is considered linked or reasonably linkable when it directly links to an individual or can be combined with other data to make identification possible. The concept of linking is important because it includes information that is reasonably linkable to an individual even if it does not directly identify that individual. In practice, the requirement that information be "linked or reasonably linkable" to an individual applies to all information that is or can be linked to an individual and also includes information that has a reasonable possibility of being linked in the future.

Other Approaches: Oregon and Washington

Oregon's definition of personal data covers "*derived data or any unique identifier* that is linked or reasonably linkable to a consumer *or to a device* that identifies, is linked to or is reasonably linkable to *one or more consumers in a household.*"[10] The specific elements of *derived data*, *unique identifier*, *device*, and *household* diverge from the most common approach. Notably, "derived data" is absent from the definition of personal data in other state privacy laws. Although the Oregon statute itself does not define *derived data*, its use of the term could be viewed

6 GDPR, Art. 4 (1).

7 Colo. Rev. Stat. § 6-1-1303(17)(a); Conn. Gen. Stat. § 42-515(26); Del. Code. tit. 6, § 12d-102; Indiana Code § 24-15-2-19 (effective Jan. 1, 2026); Iowa Code § 715D.1(18); Ky. Rev. Stat. § 367.3611(19) (effective Jan. 1, 2026); Md. Code, Com. Law § 14-4701(w) (effective Oct. 1, 2025); Minn. Stat. § 325M.11(p); Mont. Code § 30-14-2802(15) (to be renumbered as subsection (19) effective Oct. 1, 2025); N.H. Rev. Stat. Ann. § 507-H:1(XIX); N.J. Rev. Stat. § 56:8-166.4; R.I. Gen. Laws § 6-48.1-2(18); Tenn. Code Ann. § 47-18-3201(17); and Va. Code § 59.1-575.

8 *De-identified data* includes any "data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person." As such, de-identified data is excluded from the definition of personal information with publicly available information.

9 This element represents a notable distinction from the GDPR, which includes publicly available information within the scope of covered data, as well as *pseudonymized*—but not anonymized—data. How pseudonymization and anonymization should be interpreted under the GDPR has been the focus of extensive and ongoing discussion. For more analysis of key implementation issues under the GDPR, see CIPL Report, The GDPR's First Six Years: Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement, May 2024.

10 Or. Rev. Stat. § 646A.570(13)(a) (emphasis added).

as introducing a new requirement that expands compliance obligations and individual personal data rights when inferences are made about a consumer.

Washington's My Health My Data Act (MHMDA) law has a sectoral focus by purporting to provide heighted protections for health data, but it is sometimes described as *quasi-comprehensive* due to its broad and unique definitions of covered data. While the law does indeed address *consumer health data*, it also provides a broad definition of *personal information*, defined as information that identifies or is reasonably capable of being associated or linked, directly or indirectly, with a particular consumer. *Personal information* also includes, but is not limited to, data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier.[11]

MHMDA's definition of *consumer health data* arguably creates ambiguity by including information derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning). Similarly, the law's definition of *reproductive or sexual health information* includes information "derived, extrapolated, or inferred, including from nonhealth information (such as proxy, derivative, inferred, emergent, or algorithmic data)." Information *inferred* from nonhealth information can encompass a broad scope of personal information. The statute's reference to *algorithmic data* is novel and is not a data type that is typically found in comprehensive privacy laws.

An Outlier: California

Under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, the term *personal information* is defined as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly", with a particular consumer or household.[12] California's definition of personal information specifically includes identifiers,[13] commercial information, biometric information, internet or other electronic network information, geolocation data, audio, sensory information,[14] professional or employment-related information, education information, information reflecting a consumer's preferences, and any sensitive personal information.[15] The use of the terms *relates to*, *describes*, and *reasonably capable of being associated with* are also unique to California.

In 2024, the CCPA was amended to assert that personal information can exist in various formats, including "artificial intelligence systems that are capable of outputting personal information." This amendment added to the a debate around the extent to which AI models can contain personal data,[16] and whether tokenized data (within AI models or systems) falls within the scope of personal information.

It is also important to note that California's Attorney General has clarified that under the CCPA, "internally generated inferences"—i.e., inferences that a business holds about a consumer generated internally by the business—constitute personal information within the meaning of the CCPA and must be disclosed to the consumer on request, unless a business can demonstrate that a statutory exception applies.[17]

11 Wash. Rev. Code 19.373.010(18).

12 Cal. Civ. Code § 1798.140(v)(1).

13 Under CCPA, the term *identifiers* includes the real name, alias, postal address, unique identifier, online identifier, internet protocol (IP) address, email address, account name, social security number, driver's license number, passport number, or any other similar identifiers.

14 Audio, electronic, visual, thermal, olfactory, or similar information.

15 Cal. Civ. Code § 1798.140(v)(1)(A)-(L).

16 *See*, e.g., the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) *Large Language Models and Personal Data* (July 15, 2024), col

17 See California Office of the Attorney General, 105 Ops. Cal. Atty. Gen. 26 (March 10, 2022).

Exclusions

At the time of this writing, every state's definition of personal information excludes publicly available information and de-identified data.

Publicly available information, however, is not uniformly defined. It can refer to information that is lawfully made available from federal, state, or local government records, and/or to information that a controller has a reasonable basis to believe has lawfully been made available to the general public.

De-identified data includes any data that cannot reasonably be linked to an identified or identifiable natural person, or to a device linked to such person.

Indiana, Iowa, Tennessee, and Utah also exclude *aggregated data (or consumer information)* from their definitions of *personal data*.[18]

18 Indiana Code § 24-15-2-19(b)(2); Iowa Code § 715D.1(18); Tenn. Code Ann. § 47-18-3302(17); and Utah Code § 13-61-101(24)(b).

3. The Inclusion of Sensitive Data

The concept of *sensitive data* originates from international human rights laws and data protection frameworks that seek to protect individual fundamental rights against harms stemming from the misuse of personal information. The GDPR classifies the following types of data as sensitive: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; and data concerning a person's sex life or sexual orientation.[19]

In the context of US state comprehensive privacy laws, the term refers to personal information that is deemed to pose higher risks to individuals if used inappropriately, thus requiring a higher level of protection than other types of data. For most states, this means that covered entities must obtain consent before the collection and processing of such data.

Most Common Approach

The categories of information below are universally recognized as sensitive across all US state privacy laws

Personal data *revealing or indicating*:

- racial or ethnic origin
- religious beliefs
- sexual orientation, sex life, or sexuality[20]
- citizenship or immigration/citizenship status[21]
- genetic or biometric data

Most state laws include the language "personal data *revealing*" (emphasis added) in their definitions of *sensitive data*, but Colorado is the only state that explicitly defines the term *revealing*.[22] The Colorado Privacy Act's corresponding regulations define *revealing* as including sensitive data inferences, which, in turn, is defined to mean "inferences made by a Controller based on Personal Data, alone or in combination with other data, which are used to indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status."[23]

19 GDPR, Art. 9(1). The GDPR uses the term "special categories of personal data."

20 Texas is the only state that lists *sexuality* as a category of sensitive data. Tex. Bus. & Com. Code § 541.001(29)(A). The Texas law does not define the term *sexuality*, but it can be interpreted more broadly to include sexual orientation among other things.

21 All states recognize *citizenship or immigration* status except Colorado who lists "citizenship or citizenship status" as sensitive.

22 *See* Colorado Privacy Act Rules, 4 CCR 904-3-2.02.

23 *Id.*

Other Approaches

The following categories of information are recognized as sensitive by most states (with the exceptions noted below):

- mental or physical health condition or diagnosis (not mentioned in Maryland's law)
- personal data from a known child (not mentioned in laws from California and Utah)
- precise geolocation data (not mentioned in Colorado's law)

The following categories of information are recognized as sensitive only by the states noted below:

- national origin (Maryland and Oregon)
- status as transgender or nonbinary (Connecticut, Delaware, Maryland, New Jersey, and Oregon)
- status as the victim of a crime (Connecticut and Oregon)
- finance-related information (California, Connecticut, and New Jersey)
- neural data[24] (California and Connecticut)
- biological data (including neural data) [25] (Colorado)
- government-issued identification number (Connecticut)
- disability or treatment (Connecticut)

An Outlier: California

California is the only state that recognizes the following categories as sensitive:

- philosophical beliefs
- Social Security numbers
- driver's license numbers
- state ID or passport numbers
- union membership
- contents of a consumer's mail, email or text messages[26]

Please see the Appendix for a graphic comparing categories of sensitive data across the states.

The Federal Approach

While Congress has yet to adopt a federal privacy law, the concept of sensitive data under state laws intersects with definitions under a rule recently issued by the US Department of Justice that has substantial implications for organizations' data governance practices.

On February 28, 2024, President Biden issued Executive Order 14117 (EO 14117) (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern), which directed the Attorney General to issue regulations that prohibit or otherwise restrict transactions that involve government-related data or bulk US sensitive personal data posing a national security risk.[27] The Department of Justice issued

24 California defines neural data as information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information." However, in Connecticut, "[n]eural data means any information that is generated by measuring the activity of an individual's central nervous system."

25 Biological data, which is data generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or activities or of an individual's body or bodily functions, which data is used or intended to be used, in fly or in combination with other personal data, for identification purposes; and "neural data," which is information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device.

26 Unless a business is the intended recipient of the communication.

27 Executive Office of the President, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, 89 FR 15421 (Feb. 28, 2024).

its Final Rule on January 8, 2025 (Final Rule).[28] Its "Data Security Program"[29] went into effect, with the exception of certain due diligence, audit and reporting obligations,[30] on April 8, 2025.

The Final Rule prohibits or restricts US persons from knowingly engaging in certain *covered data transactions* that could result in access to bulk US sensitive personal data or any Government-related data by a country of concern or covered person.[31]

A *covered data transaction* is defined under the rule as any transaction that involves any access to any government-related data or bulk US sensitive personal data and that involves data brokerage, a vendor agreement, an employment agreement, or an investment agreement.[32]

The Final Rule defines the term *sensitive personal data* as "covered personal identifiers, precise geolocation data, biometric identifiers, human 'omic data,[33] personal health data, personal financial data, or any combination thereof."[34]

The Final Rule specifies that *sensitive personal data* does not include:

1. Public or nonpublic data that does not relate to an individual, including such data that meets the definition of a "trade secret" or "proprietary information";
2. Data that is, at the time of the transaction, "lawfully available to the public from a Federal, State, or local government record…or in widely distributed media…";
3. Personal communications; and
4. Information or informational materials and ordinarily associated metadata or metadata reasonably necessary to enable the transmission or dissemination of such information or informational materials.[35]

Organizations that have built privacy programs around compliance with US state laws will need to examine carefully how their obligations under those statutes compare to, and interact with, those under the Final Rule. They also must be mindful of interactions with other federal, sectoral privacy laws, some of which are addressed through specific exemptions in the state laws, as discussed further below. These laws include:

The Gramm Leach Bliley Act (GLBA) (15 USC § 6802(a) et seq.) governs the protection of personal information in the hands of banks, insurance companies and other companies in the financial service industry. This statute protects Non-Public Personal Information (NPI), which includes any information that a financial service company collects from its customers in connection with the provision of its services.

HIPAA, or the Health Insurance Portability and Accountability Act of 1996, as amended (29 USC § 1181 et seq.) protects information held by a covered entity that concerns health status, provision of healthcare or

28 National Security Division, US Department of Justice, Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 FR 1636 (Jan 8, 2025).

29 National Security Division, US Department of Justice, Data Security Program, accessed July 16, 2025.

30 These obligations are effective October 5, 2025.

31 See 90 FR 1636 at 1639 (citing National Security Division, US Department of Justice, Provisions Pertaining to Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 89 FR 86116 at 86118 (Oct. 29, 2024)).

32 90 FR 1636 at 1708 (citing 89 FR 86116 at 86121); 28 CFR § 202.21

33 The term *human 'omic data* means data generated from humans that characterizes or quantifies human biological molecule(s), such as human genomic data, epigenomic data, proteomic data, transcriptomic data, microbiomics data, or metabolomic data, as further defined by regulations issued by the Attorney General.

34 90 FR 1636 at 1716; 28 CFR § 202.249. See also National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 FR 15780 (Mar. 5, 2024); and 90 FR at 1649 (Jan. 8, 2025).

35 See 89 FR 86122.

payment for healthcare that can be linked to an individual. Protected health information (PHI) is defined as any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

The Family Educational Rights and Privacy Act (FERPA) (20 USC. § 1232g) protects the confidentiality of student educational records. It applies to any public or private elementary, secondary, or post-secondary school and any state or local education agency that receives federal funds under a program administered by the Secretary of Education. There are two essential criteria for a document to be considered part of an *education record* under FERPA: the record must "directly relate" to a student, and must be "maintained by an educational agency or institution or by a person acting for such agency or institution."

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (15 USC § 1681) protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services. This law restricts use of information with a bearing on an individual's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to determine eligibility for credit, employment or insurance.

Children's Online Privacy Protection Act (COPPA) (15 USC. §§ 6501-6506), a US federal law enacted in 1998 and enforced by the Federal Trade Commission (FTC) that protects the online privacy of children under 13. It requires websites and online services to obtain parental consent before collecting, using, or sharing personal information from children under 13. Personal information under the context of this law means individually identifiable information about an individual collected online.

The Drivers Privacy Protection Act (DPPA), 18 USC. § 2721, was originally enacted in 1994 to protect the privacy of personal information assembled by State Departments of Motor Vehicles (DMVs). The DPPA prohibits the release or use by any State DMV (or any officer, employee, or contractor thereof) of personal information about an individual obtained by the department in connection with a motor vehicle record.

4. Exemptions

States generally have two categories of exemptions that effectuate exclusions from the scope of their privacy laws: data-level exemptions and entity-level exemptions. A data-level exemption applies to a certain type of data, such as data collected in the employment context, the processing of which is not covered by the statute, even though the organization processing that data is otherwise subject to the law. In contrast, an entity-level exemption removes the organization itself (such as a non-profit) from the scope of the law, regardless of the data it is processing.[36]

Most Common Approach

All state-level comprehensive privacy laws exclude from their scope certain entities, such as government agencies, non-profits, or institutions of higher education. Most states also exclude entities or data that are already subject to sectoral privacy legislation under federal law, such as GLBA, HIPAA, FERPA, FCRA, COPPA, and DPPA.

The following categories of information are exempted at the data-level across all US state privacy laws (with the exceptions noted below):

- Employee data (except California)
- Data covered under FCRA
- Data covered under DPPA
- Data covered under FERPA (except New Jersey)

Aside from California, all states exempt employee and business-to-business data.[37] All states have either a data-level exemption and/or entity-level exemption for GLBA and HIPAA, as well as data-level exemptions for data covered by FCRA and DPPA. All states except New Jersey exempt student education record data under FERPA.

Other Approaches

Most states exempt the following entities from the scope of their laws, with the exceptions noted below:

- Government (except Colorado)
- Nonprofits (except Colorado, Delaware, Minnesota, New Jersey, and Oregon)
- Higher education (except California, Delaware, Maryland, New Jersey, and Oregon)

Only Colorado, Connecticut, Delaware, Maryland, Montana, New Hampshire, and Rhode Island exempt national securities associations.

36 US state privacy laws apply various thresholds regarding their scope and applicability, such as whether an entity's revenue meets a specific threshold or whether it is generated from the sale of personal data, the volume of personal data processed, and number of residents whose data processed or sold.

37 Small businesses, as defined by the US Small Business Administration, are exempt from state privacy laws in Nebraska, Minnesota, and Texas. A number of states also provide exemptions for entities below thresholds of either revenue or the number of consumers' data processed or sold.

Figure 1: State Privacy Law Exemptions for Federal Obligations

	GLBA	HIPAA	FERPA	FCRA	DPPA
California	Data-level	Data-level	Data-level	Data-level	Data-level
Colorado	Entity-level & data level	Data-level	Data-level	Data-level	Data-level
Connecticut	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Delaware	Entity-level	Data-level	Data-level	Data-level	Data-level
Florida	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Indiana	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Iowa	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Kentucky	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Maryland	Entity-level	Data-level	Data-level	Data-level	Data-level
Minnesota	Data-level	Data-level	Data-level	Data-level	Data-level
Montana	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Nebraska	Entity-level	Entity-level & data level	Data-level	Data-level	Data-level
New Hampshire	Entity-level & data level	Data-level	Data-level	Data-level	Data-level
New Jersey	Entity-level	Data-level	No exemption	Data-level	Data-level
Oregon	Data-level	Data-level	Data-level	Data-level	Data-level
Rhode Island	Entity-level & data level	Data-level	Data-level	Data-level	Data-level
Tennessee	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Texas	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Utah	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level
Virginia	Entity-level & data level	Entity-level & data level	Data-level	Data-level	Data-level

Data-level exemption
Entity-level exemption
Entity-level & data level exemptions
No exemption

Source: The Centre for Information Policy Leadership

5. Policy Considerations

The Limitations of *Sensitive* Data

While a robust data privacy law is essential to ensure consumer trust and safeguard consumer rights, not all regulatory obligations yield proportional benefits to consumers. This is especially relevant in the context of defining covered and *sensitive* data, where extensive lists of data types may not reflect context-specific or use-based benefits and harms. While designating certain categories of personal information as *sensitive* is intended to afford heightened protections that mitigate privacy and security risks, this practice has notable conceptual and operational limitations. Indeed, many types of personal data can become sensitive depending on the circumstances, so it is important to assess data uses in context. This is particularly the case when nonsensitive data can be used to infer sensitive information about individuals. An example of this would be when information about a user's reading habits could lead to inferences about that individual's religion, mental health, or race.[38] Data may be benign in one context and potentially harmful in another, depending on factors such as the purpose, use, processing, and sharing of the data. Similarly, certain uses of *sensitive* data may be benign and not warrant heightened protections in some contexts. Privacy laws should recognize the context-specific nature of data sensitivity and focus on addressing consumer protections in a manner that accounts for factors such as the intended use. This is especially important for AI, as the training of models often requires use of rich and diverse datasets to ensure model quality.[39]

The Link to Data Minimization

The definitions of covered and sensitive data are especially important given their role in determining which data held by organizations are subject data to minimization provisions.

Data minimization is a longstanding element of data protection globally and a core element in many US state privacy laws. Increased attention to data minimization in recent years reflects growing concerns about the risks associated with unnecessary or excessive data collection.[40] CIPL has written about the importance of architecting and interpreting data minimization principles carefully so as to support innovative and beneficial development of AI while protecting individuals' privacy, and we have noted that the volumes of data needed to be collected for legitimate purposes can vary substantially. Necessity should be interpreted to permit the processing of large volumes of personal data where it is essential to achieve a legitimate purpose, such as the proper functioning of an AI model, mitigating bias, or improving fairness.[41]

38 Solove, Daniel J., *Data Is What Data Does: Regulating Based on Harm And Risk Instead of Sensitive Data*, (2024) Northwestern University Law Review, Vol. 118. No. 4 at 1090.

39 CIPL, Rethinking Sensitive Data in the Age of AI, September 2025.

40 See CIPL Report, Data Minimization in the United States' Emerging Privacy Landscape: Comparative Analysis and Exploration of Potential Effects, August 16, 2024. CIPL has also argued that the principle of data minimization must be interpreted carefully so as to support innovative and beneficial development and deployment of AI. CIPL AI First Report, Artificial Intelligence and Data Protection in Tension, October 29, 2018, CIPL AI Second Report, Hard Issues and Practical Solutions, February 27, 2020, and CIPL Report, Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators, December 6, 2024.

41 CIPL White Paper, Reconciling AI with the Data Minimization Principle: Bridging the Innovation and Privacy Gap (forthcoming).

Most US state privacy laws impose a duty of data minimization, limiting the collection of personal data to what is *adequate, relevant, and reasonably necessary* in relation to the purposes for which such data is processed, as disclosed to an individual. Under these laws, covered entities are not to process personal information for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes, unless the business obtains an individual's consent. The obligations with respect to both collection and processing require that businesses identify and disclose processing purposes during the initial data collection.[42]

Maryland's comprehensive privacy law—as well as laws with narrower scope, such as Washington state's My Health My Data Act—take a stricter approach, with especially restrictive rules for sensitive data. For example, under Maryland's law, controllers are prohibited from selling sensitive personal data and can only collect, process, or share such data if it is *strictly necessary* to provide or maintain a requested product or service. Many businesses have found Maryland's standard particularly challenging to implement.

Relevance of Data vs. Entity-Level Protections

The distinction between data-level and entity-level exemptions has important compliance implications because organizations need to identify whether they are a covered entity and whether the data they are using is covered. Such considerations are vital to internal data governance and compliance measures.

Threading the needle may be especially complex for organizations not subject to privacy laws in states that contain entity-level exemptions but are nevertheless subject to laws in other states that contain a narrower, data-level exemption. In other words, an organization entirely exempt from one state law may remain subject to another state's law with respect to all non-exempt personal data it processes.

As additional state (and federal) legislators consider the relevance of data- vs. entity-level exemptions, they should be alert to the potential impact of additional new inconsistencies across laws.

Differing Definitions of Personal Data Under Sectoral Laws

A byproduct of the current US landscape, which features both federal sectoral laws and state privacy laws, is the challenge presented by diverse definitions of covered information. As mentioned above, comprehensive state privacy laws generally define personal information in industry-neutral terms that encompass any data reasonably linkable to an individual (or household), but federal sectoral laws, restrict their scope to narrowly defined categories, such as *protected health information* or *education records*, which are applicable only to certain regulated entities. This difference creates legal uncertainty for entities with hybrid business models. Such a fragmented approach increases the likelihood of confusion for organizations building compliance programs—as well as for enforcers of the conflicting statutes. The prospect for confusion and unnecessary complexity points to the merits of harmonized definitions under a future federal privacy law, as CIPL has discussed in depth elsewhere.[43]

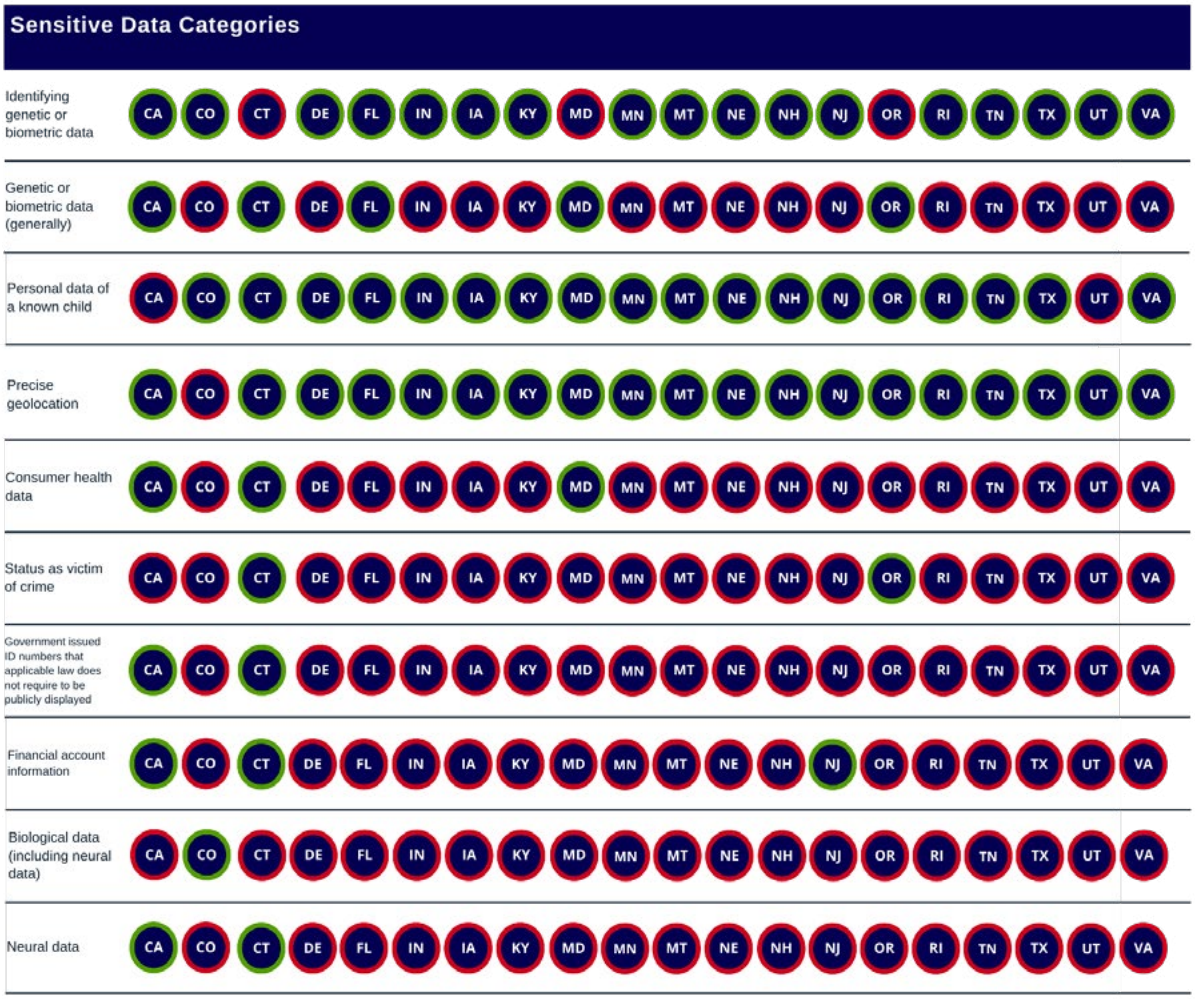
42 CIPL Report, Comparison of US State Privacy Laws: Data Protection Assessments, February 8, 2024.
43 CIPL, Ten Principles for a US Privacy Law, April 2025.

6. Conclusion

The patchwork of definitions and classifications of personal information across US state privacy laws has created operational and compliance challenges for organizations who handle diverse data types across different sectors and jurisdictions. The lack alignment in definition and obligations complicates organizations' risk assessments, accountability mechanisms, and the design of privacy programs, monopolizing organizations' limited resources away from innovation. For policymakers and organizations, harmonizing the definitions of covered and sensitive data, accounting for the context-specific nature of data sensitivity by focusing on intended use, and tying regulatory obligations to actual risk of harm should be a central focus. Clear, consistent rules in this space will ensure consumer clarity, support responsible data use, and facilitate the safe development and deployment of emerging technologies, such as AI.

Appendix: Categories of Sensitive Data Under US State Laws

Sensitive Data Categories																				
Racial or ethnic origin	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
National origin	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Religious beliefs	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Mental of physical health diagnosis	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Mental or physical health condition	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Mental or physical health treatment	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Mental or physical disability	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Medical history	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Sexual orientation	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Sex life	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Sexuality	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Status as transgender or non-binary	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Citizenship and immigration/citizenship status	CA	CO	CT	DE	FL	IN	IA	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA


Sensitive Data Categories
Identifying genetic or biometric data
Genetic or biometric data (generally)
Personal data of a known child
Precise geolocation
Consumer health data
Status as victim of crime
Government issued ID numbers that applicable law does not require to be publicly displayed
Financial account information
Biological data (including neural data)
Neural data
CA CO CT DE FL IN IA KY MD MN MT NE NH NJ OR RI TN TX UT VA

Source: Centre for Information Policy Leadership

About the Centre for Information Policy Leadership

The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

For more information, please see CIPL's website at

http://www.informationpolicycentre.com/

DC Office
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London Office
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels Office
Avenue des Arts 47-49
1000 Brussels
+32 2 643 58 00

© 2025 Centre for Information Policy Leadership. All Rights Reserved.

25509.1025.R1