REPORT

US POLICY

Anatomy of State Comprehensive Privacy Law

Surveying the State Privacy Law Landscape and Recent Legislative Trends

FPF U.S. Legislation Report

November 2024

Jordan Francis, Policy Counsel, U.S. Legislation

FUTURE OF PRIVACY FORUM

Executive Summary

Between 2018 and 2024, nineteen U.S. states enacted comprehensive consumer privacy laws. These include privacy laws that are technology neutral, broadly applicable, and non-sectoral. This rapid adoption of privacy legislation has caused the state privacy law landscape to explode in depth and complexity as each new law iterates upon those that came before it. This report summarizes that legislative landscape and identifies the "anatomy" of state comprehensive privacy law by comparing and contrasting the two prevailing models for state laws, focusing on the commonalities and differences in the laws' core components. These core components of a comprehensive privacy law include: definitions of covered entities (controllers and processors) and covered data (personal data and sensitive data); individual rights of access, correction, portability, deletion, and both opt-in and opt-out requirements for certain uses of personal data; business obligations such as transparency, data minimization, and data security; and enforcement.

Many of the elements of privacy laws explored in this report (e.g., data minimization or the scope of sensitive data) are broad enough that entire reports could be written about those issues alone. Rather than providing an exhaustive, detailed comparison as to how each state law addresses a particular issue, this report focuses on high-level similarities and differences between the various state laws, with an emphasis on highlighting "typical" language and where states have diverged from their peers in consequential ways. By framing the analysis around high-level similarities and differences, this report is designed to be an accessible "on-ramp" to the state privacy law landscape.

This report concludes by highlighting recent legislative trends, including: changes to applicability thresholds; the expanding scope of sensitive data; the emergence of substantive data minimization requirements; new heightened protections for consumer health data, adolescents' personal data, and biometrics; and new individual rights such as to be notified of specific third-party recipients of personal data and a right to contest adverse profiling decisions.

By distilling this broad landscape to identify the "anatomy" of state comprehensive privacy law, this report highlights the strong commonalities and the nuanced differences between the various laws, showing how they can exist within a common, partially-interoperable framework while also creating challenging compliance difficulties for companies within their overlapping ambits. Unless and until a federal privacy law materializes, this ever changing state landscape will continue to evolve as lawmakers iterate upon the existing frameworks and add novel obligations, rights, and exceptions to respond to changing societal, technological, and economic trends.

Acknowledgements

The author thanks Keir Lamont and Bailey Sanchez for their contributions to this report.

Table of Contents

I. Overview of the State Landscape

Between 2018 and 2024, nineteen U.S. states passed comprehensive privacy laws. This report uses the term "comprehensive privacy laws" to refer to broadly applicable, non-sectoral, "consumer" privacy laws that establish baseline rights and responsibilities for the collection, use, and sharing of personal data[1] throughout the economy. These laws are "consumer" privacy laws in that they regulate the collection, use, and sharing of personal data by non-government organizations and they typically exclude employee data or data collected in a business-to-business context. For the purposes of this report, comprehensive privacy laws do not include significant sectoral laws, such as Washington's My Health My Data Act, or youth codes, such as the California Age-Appropriate Design Code, although many of these sectoral laws may have broad scopes similar, but not identical, to a comprehensive law, and many comprehensive privacy laws include heightened protections for data covered by sectoral laws, such as health data and children's data.[2] This report likewise does not consider the Florida Digital Bill of Rights amongst the comprehensive privacy laws because of its narrow applicability thresholds,[3] but it is included in Figure 1 below and in Table 1 (Appendix) for completeness.

This report aims to provide a short and accessible summary of the state comprehensive privacy law landscape, contrast the two prevailing regimes, and identify the common core components of these laws. See Table 1 (Appendix) for links to these state laws and FPF's prior analysis of each.

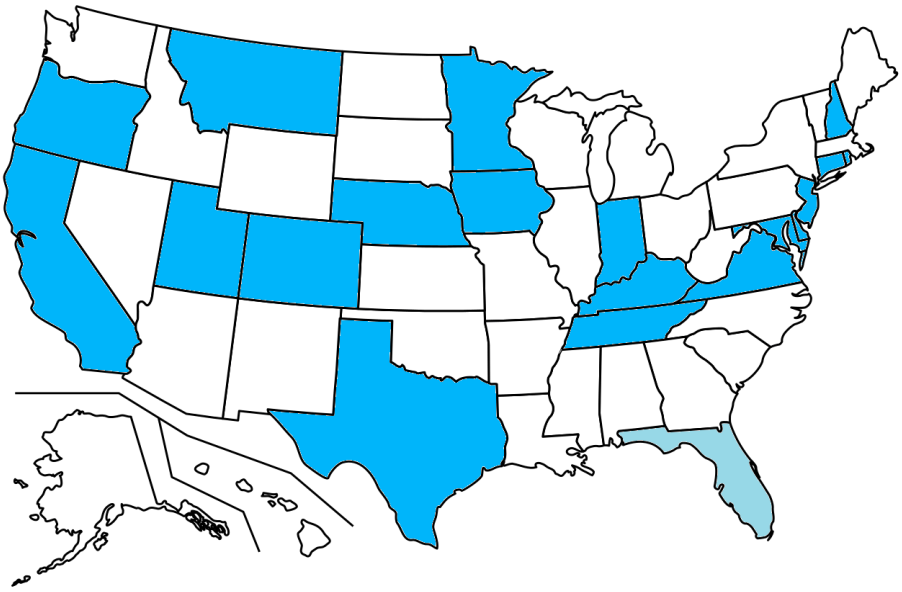

Figure 1. Map of States with Comprehensive Privacy Laws as of September 2024

[1] Of the nineteen U.S. state comprehensive privacy laws, seventeen laws use the term "personal data" whereas California's and Tennessee's laws use the term "personal information." This report defaults to the term "personal data" unless talking about one of those states specifically.
[2] Other privacy-focused organizations, such as the IAPP, have made similar decisions as to the scope of a "comprehensive" privacy law. Andrew Folks, *Defining 'Comprehensive': Florida, Washington and the Scope of State Tracking*, IAPP (Feb. 22, 2024), https://iapp.org/news/a/defining-comprehensive-florida-washington-and-the-scope-of-state-tracking.
[3] *Id.*

A. Two Competing Models: Background of the CCPA and the WPA Frameworks

There are two prevailing privacy law regimes at the state level—one that is solely represented by the ***California Consumer Privacy Act (CCPA)*** and another seen in the eighteen state laws that are based on the ***Washington Privacy Act (WPA) Framework***. At the time of publication, eighteen of the nineteen state comprehensive privacy laws are based on the WPA framework, resulting in roughly 39 million Americans being covered by the CCPA compared to 106 million Americans being covered by variants of the WPA framework.[4]

Enacted in 2018, the CCPA was the first state comprehensive privacy law and has been credited with "catalyzing" privacy law across the U.S.[5] California was ahead of the curve in terms of legislating U.S. privacy rights, but the CCPA as originally enacted lacked provisions that are typical of global privacy laws, such as heightened protections for sensitive data, risk assessment requirements, and a right to correct inaccurate data. This could be due to the law's unique history and rushed legislative process. The CCPA started as a ballot initiative which was withdrawn when a substantially similar bill was instead passed by the California State Legislature.[6] In response to perceived weaknesses in the law, Californians approved the Consumer Privacy Rights Act (CPRA) via a 2020 ballot initiative, amending the law to add new rights and protections. The CPRA also created a new standalone privacy agency, the California Privacy Protection Agency (CPPA), which is vested with rulemaking authority. The law has been buttressed by extensive regulations over the years, by the Attorney General and later by the CPPA. This unique procedural history—existing as a ballot initiative turned bill then amended by a ballot initiative and further expanded through rulemaking—has resulted in the CCPA's various rights and obligations being a moving target in its six year history. That shifting, volatile nature of the law may have diminished its likelihood of catching on as a model framework for other states to enact.[7] In the absence of a stable and replicable "California model," state policymakers have looked elsewhere for inspiration.

---

[4] Calculated (excluding Florida) using 2023 population values from the following table: U.S. Dept. Ag., *Population*, https://data.ers.usda.gov/reports.aspx?ID=17827 (last visited July 29, 2024).

[5] Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1762–93 (2021) (examining proposed privacy legislation, noting similarities to the CCPA, and concluding that U.S. states considering privacy legislation were responding more to the CCPA than the European Union's General Data Protection Regulation (GDPR)).

[6] Katelyn Ringrose & Jeremy Greenberg, *California Privacy Legislation: A Timeline of Key Events*, FPF (July 1, 2020), https://fpf.org/wp-content/uploads/2020/07/California-Privacy-Legislation_-A-Timeline-of-Key-Events.pdf.

[7] Another possible contributing factor as to why the "California model" never caught on was coordinated lobbying efforts that promoted the WPA framework. *See* Brendan Bordelon & Alfred Ng, *Tech Lobbyists Are Running the Table on State Privacy Laws*, POLITICO (Aug. 16, 2023), https://www.politico.com/news/2023/08/16/tech-lobbyists-state-privacy-laws-00111363; Alfred Ng, *The Man Quietly Rewriting American Privacy Law*, POLITICO (Sept. 18, 2024), https://www.politico.com/news/2024/09/17/andrew-kingman-data-privacy-lobbying-00179630.

The Washington Privacy Act (WPA) was a bill introduced in Washington State in 2019 and multiple years thereafter.[8] It was never enacted, however, largely due to debates over enforcement mechanisms—particularly whether to include a private right of action.[9] Nevertheless, the WPA was strengthened over the multiple years it was introduced and ultimately became a model framework for privacy legislation in other states.[10] When stakeholders discuss the "Virginia model,"[11] "Colorado model,"[12] or "Connecticut model,"[13] they are referring to different iterations of the WPA framework. Virginia was the first state to enact a law based on the WPA framework, and Colorado and Connecticut adopted that same model, but incorporated strong, privacy-protective elements from the CCPA, such as a broad definition of "sale,"[14] recognition of opt-out preference signals, and heightened protections for adolescents. This report refers to the WPA as a *framework* because it represents a set of baseline principles, terms, and structure that the majority of states have incorporated into their privacy laws. However, while these laws share key definitions and a common framework, they also vary significantly in scope, individual rights, and business obligations.

Thus, while nearly half of all Americans now enjoy comprehensive privacy protections under one of these 19 laws—or will once these laws take effect, cure periods expire, necessary regulations are promulgated, and attorneys general begin enforcing them—these rights and protections vary by geography. High-level differences between the CCPA and the WPA framework include:

	CCPA	WPA Framework
Enforcement	Attorney General and California Privacy Protection Agency share authority	Enforcement solely by Attorney General

[8] *Senate Passes Carlyle's Washington Privacy Act*, SENATE DEMOCRATS (Mar. 6, 2019), https://senatedemocrats.wa.gov/blog/2019/03/06/senate-passes-carlyles-washington-privacy-act.
[9] Natasha G. Kohne & Anthony T. Pierce, *Washington State Lawmakers Divided Over Private Right of Action and Other Relief in Dueling Data Privacy Bills*, AKIN GUMP (Feb. 18, 2020), https://www.akingump.com/en/insights/alerts/washington-lawmakers-divided-over-private-right-of-action-and.
[10] Stacey Gray, Pollyanna Sanderson & Katelyn Ringrose, *Comparison of the Proposed 2020 Washington Privacy Act (SSB-6281) to: GDPR, CCPA, California Ballot Initiative, and the 2019 WA Proposal*, FPF (Feb. 12, 2020), https://fpf.org/wp-content/uploads/2020/02/fpf_comparison_of_wa_ssb-6281_to_gdpr__ccpa__cpra__and_2019_version_-_v1.0_feb_12_2020-1.pdf.
[11] *E.g.*, Max Rieper, *In the Absence of Federal Action, States Continue to Lead on Comprehensive Privacy Legislation*, MULTISTATE (July 21, 2023), https://www.multistate.us/insider/2023/7/21/in-the-absence-of-federal-action-states-continue-to-lead-on-comprehensive-privacy-legislation.
[12] *E.g.*, Robert Blamires, Clayton Northouse, Austin L. Anderson & Jennifer Howes, *Oregon and Delaware Join the Surge of US States Enacting General Privacy Legislation*, GLOBAL PRIVACY BLOG (Sept. 6, 2023), https://www.globalprivacyblog.com/2023/09/oregon-and-delaware-join-the-surge-of-us-states-enacting-general-privacy-legislation.
[13] *E.g.*, Scott Medintz, *Does Your State Care About Your Digital Privacy?*, Consumer Reports (June 21, 2024), https://www.consumerreports.org/electronics/privacy/does-your-state-care-about-your-digital-privacy-a3262142390.
[14] *Compare* Va. Code Ann. § 59.1-575 (2023) (defining sale as "the exchange of personal data for monetary consideration by the controller to a third party"), *with* Colo. Rev. Stat. § 6-1-1303(23)(a) (2023) (defining sale as "the exchange of personal data for monetary or other valuable consideration").

	CCPA	WPA Framework
Sensitive Data	Opt-out: Individuals can direct the business to limit its use of their sensitive personal information to uses that are necessary to provide the goods or services reasonably expected by the average individual, or to perform certain "business purposes"	Opt-in: Businesses must obtain opt-in consent (freely given, specific, informed, unambiguous) to process sensitive data
Rulemaking	Broad authority, with significant rights and obligations to be finalized in regulations (e.g., automated decisionmaking technology opt-out rights, risk assessments, cybersecurity audits)	None, as provisions are largely self-executing. Exceptions: Explicit rulemaking granted in Colorado, Florida, New Jersey
Scope of Personal Data	Applies to "personal information," which includes employee and B2B data	Only covers 'personal data' in consumer context
Regulated Entities	Business, Service Provider, Contractor, Third Party	Controller, Processor
Private Rights of Action	Narrow PRA, only for data breaches	None

Table 2. At a Glance: CCPA v. WPA Framework

* * *

The following section identifies and summarizes the core definitions, rights, and obligations of the WPA framework and the CCPA. Although the CCPA predates the WPA framework, this analysis begins with the WPA framework because it is a framework that has been adapted and enacted in multiple states. The WPA framework is also simpler than the CCPA—due to the CCPA's complex drafting history, ongoing modifications and regulations—making the WPA framework a better starting place for an introductory overview of the state comprehensive privacy law landscape. The subsequent analysis of the CCPA focuses on that law's differences from the WPA framework.

B. The WPA Framework

This section deconstructs the Washington Privacy Act (WPA) framework into its core elements that are common across enacted laws and indicative of legislation based on this model. The WPA framework is built around five core components which constitute a comprehensive privacy law: (1) covered entities; (2) covered data; (3) individual ("consumer") rights; (4) business obligations; and (5) enforcement by the attorney general. The following subsections introduce these core concepts at a high level and discuss common provisions and language. Note that actual requirements vary between the different laws, and this analysis omits many exemptions, limitations, qualifications, and other nuances.

1. Covered Entities

Who's in scope? Most statutory responsibilities are allocated by role between two categories of covered entities—***controllers*** and ***processors***. The vast majority of obligations apply to ***controllers***, who are individuals or entities that alone or jointly with others determine the purpose

and means of processing personal data. To be a controller, entities have to meet a jurisdictional requirement and a processing threshold. The jurisdictional hook requires a connection to the state—an entity must conduct business in the state or produce products or services targeted to the state's residents. The processing threshold requires that the entity process the personal data of a minimum number of state residents. There is typically a default threshold based purely on the number of affected individuals (e.g., 100K) and a lower threshold (e.g., 25K) that applies if the entity derives a certain percentage of its revenue (e.g., 20%) from selling personal data. Those thresholds vary state-to-state, and the numbers used as examples above are common but not universal.

Some obligations flow from controllers to ***processors***, the individuals or legal entities who process personal data on behalf of a controller. Processors are typically required to adhere to a controller's instructions, assist the controller in meeting the controller's obligations under the law (e.g., in fulfilling individual rights requests), and enter into contracts satisfying several statutory criteria. Processors may carry out limited sets of operations on a limited set of data on behalf of a controller, which warrants oversight and some obligations under the law, but processors may not be in a position to independently ensure the full suite of rights and responsibilities under the law. For example, since processors typically do not directly interact with individuals nor control the purpose or means of processing, they may not be in position to provide required notices to individuals or determine the underlying lawfulness of a specific processing activity.[15]

Who's not in scope? WPA-style laws typically exclude a wide array of businesses and organizations. The applicability thresholds discussed above are designed to exclude many ***small businesses*** from coverage under the law. Tying that threshold to the number of individuals whose personal data are processed, however, may still bring extremely data-intensive small businesses and start-ups into scope. Another category of entities almost universally excluded are ***government entities***. Definitions vary, but government entities usually encompasses any political subdivision of the state. Two categories of entities that are often, but not always, exempted are ***nonprofits*** and ***institutions of higher education***. The last notable category of exempted entities are those persons or entities that are subject to other, specified privacy laws. These are ***entity-level exemptions***, and may include organizations and/or data subject to Title V of the Gramm-Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and various other state and federal laws.[16] The motivation for including entity-level exemptions is to avoid subjecting organizations to overlapping and potentially conflicting requirements on the same topic.

[15] The controller-processor distinction and requirements, such as entering into a processor contract, comes from GDPR. *See* Pollyanna Sanderson, *It's Raining Privacy Bills: An Overview of the Washington State Privacy Act and other Introduced Bills*, FPF (Jan. 13, 2020), https://fpf.org/blog/its-raining-privacy-bills-an-overview-of-the-washington-state-privacy-act-and-other-introduced-bills.

[16] An alternative to entity-level exemptions are ***data-level exemptions***, which exempt only data subject to specified privacy laws. *Infra* Part I.B.2.

2. Covered Data

What data is in scope? Laws typically apply to processing of ***personal data***, which is any information linked or reasonably linkable to an identified or identifiable individual ("consumer").[17] Some states have expanded the definition of personal data to include data linked or linkable to (1) devices that are in turn linked or linkable to individuals and/or (2) individuals in a household.[18] These laws also include heightened protections for ***sensitive data***, a defined subcategory of personal data the breadth of which differs state-to-state.[19] Common categories of sensitive data include:

- Personal data revealing certain characteristics (e.g., racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, citizenship or immigration status);
- Biometric or genetic data processed for unique identification;
- Personal data collected from a known child; and
- Precise geolocation data (that identifies an individual within a radius of 1,750).[20]

What data isn't in scope? To satisfy potential intrusions on First Amendment protections, these laws typically exclude ***publicly available information*** from coverage.[21] Definitions of publicly available information vary state-to-state, but common categories include information lawfully made available from government records, information lawfully made available in widely distributed media, and information a controller has a reasonable basis to believe an individual lawfully made available to the general public. There are ***data-level exemptions***, providing that the law does not apply to information subject to certain state or federal privacy laws such as GLBA, HIPAA, FERPA, FCRA, and more. Like with entity-level exemptions, the purpose of data-level exemptions is to avoid subjecting organizations to overlapping and potentially

---

[17] This definition bears a strong resemblance to that under the GDPR. GDPR, art. (4)(1) ("personal data' means any information relating to an identified or identifiable natural person ('data subject')"). Note that these state laws typically use the term "consumer" so as to clarify that personal data must relate to an individual acting in a personal, non-employment context. This report instead uses the term "individual," unless quoting a given law.

[18] *E.g.*, Or. Rev. Stat. § 646A.570(13)(a) (2023) (defining personal data as "data, derived data or any unique identifier that is linked to or is 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").

[19] For an "omnibus" definition of sensitive data under state comprehensive privacy laws, see Keir Lamont & Jordan Francis, *The Expanding Scope of "Sensitive Data" Across US State Privacy Laws*, TECH POL'Y PRESS (Mar. 7, 2024), https://www.techpolicy.press/the-expanding-scope-of-sensitive-data-across-us-state-privacy-laws; *see also infra* Table 5 (Appendix) for a more up-to-date list of sensitive data elements.

[20] In California, this is defined as 1,850 feet. In Minnesota, it is defined by reference to decimal points of latitude/longitude coordinates. In Colorado, precise geolocation data is only considered sensitive data if it gives rise to an inference of sensitive data.

[21] *See* Margot E. Kaminski & Scott Skinner-Thompson, *Free Speech Isn't a Free Pass for Privacy Violations*, SLATE (Mar. 9, 2020), https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html; David Stauss & Stacey Weber, *How Do the CPRA, CPA & VCDPA Treat Publicly Available Information?*, BYTE BACK LAW (Jan. 27, 2022), https://www.bytebacklaw.com/2022/01/how-do-the-cpra-cpa-vcdpa-treat-publicly-available-information (noting that the CPRA ballot initiative expanded the CCPA's "publicly available information" exception in response to First Amendment concerns).

conflicting requirements on the same topic. Laws also typically have full and partial exemptions for ***deidentified*** and ***pseudonymous*** data, respectively, whereby deidentified data is no longer considered personal data but pseudonymous data enjoys some exemptions from various rights and obligations.

Deidentified data: Typically defined as data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, provided that the controller in possession of the data (1) takes reasonable measures to ensure that the data cannot be associated with an individual, (2) publicly commits to process that data only in a deidentified fashion and not attempt to reidentify it, and (3) contractually obligates any recipients of such data to satisfy the above criteria.[22] The onward confidentiality requirement is important for safeguarding against reidentification.

Pseudonymous data: Typically defined as personal data that cannot be attributed to a specific individual without the use of additional information, so long as that additional information is (1) kept separately and (2) subject to appropriate technical and organizational safeguards to ensure that it is not attributed to an identified or identifiable individual.[23]

Other Exceptions: On top of the exemptions for various entities and categories of information, these laws also typically include numerous, broad exceptions for certain common business activities. These exceptions are intended to ensure that, regardless of whether the entity or data in question is within scope of the law, privacy laws do not interfere with socially beneficial data processing activities. State privacy laws typically provide that nothing in the law shall be interpreted to restrict a controller's or processor's ability to:

- Comply with local, state, or federal laws or regulations;
- Comply with a government subpoena, summons, inquiry or investigation;
- Cooperate with law enforcement where the controller or processor has a reasonable, good faith belief that certain conduct may violate the law;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Provide a specifically requested product or service to a customer, perform a contract to which an individual is a party, or take steps, at an individual's request, prior to entering into a contract;
- Protect the vital interests of an individual;
- Prevent, detect, protect against or respond to security incidents, deceptive activities or any illegal activity;
- Preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action;

[22] *See, e.g.*, Colo. Rev. Stat. § 6-1-1303(11); Conn. Gen. Stat. § 42-515(13). *But see* Va. Code Ann. § 59.1-575 (2023) (providing a slightly narrower definition of deidentified data that omits references to inferences).
[23] *See, e.g.*, Colo. Rev. Stat. § 6-1-1303(22); Conn. Gen. Stat. § 42-515(24).

- Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an independent oversight entity that makes certain required determinations about the benefits, risks, and safeguards associated with the research;
- Assist another controller, processor or third party with any of the obligations under the law;
- Process personal data for reasons of public interest in the areas of public health, community health or population health, subject to safeguards and the responsibility of a professional subject to legal confidentiality obligations.[24]

Amongst the broadest exceptions are provisions that preserve a controller's or processor's ability to collect, use, or retain data for "internal use" to:

- Conduct internal research to develop, improve, or report products, services, or technologies;
- Effectuate a product recall;
- Identify and repair technical errors that impair existing or intended functionality; or
- Perform "internal operations" that are (1) reasonably aligned with the expectations of the individual or (2) reasonably anticipated based on the individual's existing relationship with the controller, or (3) are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by an individual or the performance of a contract to which the individual is a party.[25]

While these exceptions can be read expansively, laws also typically try to cabin their interpretation by providing that processing of personal data pursuant to one of those exceptions must be adequate, relevant and limited to what is necessary in relation to the specific purposes listed in the exceptions, that collection should take into account the nature and purpose(s) of such collection, use or retention, and that data security obligations apply to personal data processed pursuant to an exception.

3. Individual Rights

Often referred to as "consumer rights," individual rights are statutory mechanisms for individuals to exercise some control over their information relationships with controllers. Core individual rights include the rights of ***access***, ***correction***, ***portability, deletion***, and the ability to ***opt-out*** of certain processing activities. Although these rights are subject to nuanced exceptions and procedural requirements, they typically include rights to:

- Access: Confirm whether a controller is processing their personal data and access that personal data being processed;
- Correction: Correct inaccurate personal data;

[24] This list was written based on the specific exceptions in Conn. Gen. Stat. § 42-524 (2023). Specific language and inclusion/exclusion of other exceptions varies state-to-state.
[25] This language was taken from Connecticut's law as being representative of others, but there are nuances state-to-state.

- Portability: Obtain personal data in a portable format;
- Deletion: Require that a controller delete personal data in their possession; and
- Opt-out: Opt-out of certain processing activities, which typically include processing personal data for (i) targeted advertising, (ii) sale of personal data,[26] and (iii) profiling in furtherance of decisions[27] that produce "legal or similarly significant effects" concerning the individual.[28]

Controllers have operational requirements with respect to individual rights, which may require that the controller: disclose if they are selling personal data or processing personal data for targeted advertising; establish one or more context appropriate secure and reliable means for individuals to submit a rights request; verify the identity of the individual (or their authorized agent) making the request for certain rights; and more.

Another important mechanism for individuals to exercise control in information relationships, which can be thought of as either an individual right or a business obligation, is that, typically, controllers are barred from processing sensitive data unless an individual ***opts-in*** to that processing by providing freely given, specific, informed, and unambiguous consent.[29] Requiring opt-in consent for sensitive data processing is a significant distinguisher of the WPA framework from the CCPA, which is an opt-out regime with respect to sensitive data processing.[30]

---

[26] Whether the definition of "sale" is limited to exchange of personal data for only monetary consideration or also "other valuable consideration" affects the scope of this opt-out right. *Supra* fn. 14. *See also* Samuel Adams, Stacey Gray, Aaron Massey & Rob van Eijk, *Confidential Computing and Privacy: Policy Implications of Trusted Execution Environments*, at 5, FPF (July 2024), https://fpf.org/wp-content/uploads/2024/07/FPF-Confidential-Computing-Digital.pdf (discussing *California v. DoorDash, Inc* and how "access to personal data will [generally] be considered a sale when the transferring entity receives some form of benefit and the recipient is not restricted in its subsequent uses").

[27] Sometimes limited to "solely automated decisions." *E.g.*, Conn. Gen. Stat. § 42-518(a)(5)(C) (2023). It is unclear when human involvement is limited enough that a decision is "solely automated." Whether a decision must be "solely automated" to be within scope of the opt-out right may affect a controller's incentives to include a "human in the loop" of the decisionmaking process. Providing more-detailed guidance on this issue, the Colorado Privacy Act regulations create different profiling protections and obligations for decisions based on whether they are "Solely Automated Processing," "Human Reviewed Automated Processing," or "Human Involved Automated Processing." 4 Colo. Code Reg. § 904-3, Rule 2.02.

[28] Decisions that produce legal or similarly significant effects is a term of art adopted from GDPR. *See* GDPR, art. 22. In state comprehensive privacy laws, this is typically defined as including (with some variation) decisions that result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services. *E.g.*, Colo. Rev. Stat. § 6-1-1303(10) (2023). In recent years, lawmakers have introduced legislation governing AI systems that are used to make consequential decisions about individuals, and those bills have adopted the "legal or similarly significant effects" language. Tatiana Rice, Jordan Francis & Keir Lamont, *U.S. State AI Legislation: How U.S. State Policymakers Are Approaching Artificial Intelligence Regulation*, at 5–6, (Sept. 2024), https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf.

[29] This heightened consent standard is adapted from GDPR. GDPR, art. 4(11).

[30] *Infra* Part I.C.3.

There are a number of nuances with respect to individual rights under state privacy laws:

Pseudonymous Data Enjoys Partial Exemptions: Controllers are typically exempted from complying with some or all of these rights—access, correction, deletion, and portability—with respect to pseudonymous data.[31] Tennessee and Rhode Island, however, extend the pseudonymous data exemption to their rights to opt-out of targeted advertising, sale of personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects. Exempting pseudonymous data from opt-outs with respect to sale and targeted advertising can deprive individuals of key privacy protections in several ways. For example:

- It could undermine the right to opt-out of targeted advertising because the targeted advertising ecosystem largely relies on pseudonymous identifiers, such as hashed persistent identifiers or mobile advertising identifiers; and
- It might expose individuals to secondary risks because pseudonymization does not provide meaningful protection against reidentification by downstream purchasers the same way that deidentification does, because pseudonymous data does not have the same kind of backend technical and legal requirements to prevent reidentification through cross-referencing data sets. Controllers who disclose pseudonymous data are required to exercise reasonable oversight to monitor compliance with any contractual commitments,[32] but the laws in Tennessee and Rhode Island do not create an underlying requirement to impose such contractual commitments with respect to pseudonymous data in the first place.

Universal Opt-out Mechanisms (UOOMs) on the Rise: Scholars and activists have long explained that relying on controls like opt-out rights may place a significant and unrealistic burden on individuals to engage in "privacy self-management."[33] Responsive to this risk, lawmakers in recent years have started to include provisions allowing individuals to exercise some of their opt-out rights by enabling device signals, such as the global privacy control, that communicate privacy preferences on a default basis as an individual interacts with websites.[34] Twelve of the nineteen states—California, Colorado, Connecticut, Delaware, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, and Texas—require that controllers recognize UOOMs.

Right to Delete Limited with Respect to Third Party Data: States vary in how the deletion right applies to personal data obtained from a third party. For personal data obtained from a third party, the majority of states allow the controller to respond to a deletion request by either (1) retaining a record of the deletion request and the minimum data necessary for ensuring that the individual's personal data remains deleted from the controller's records and not using that retained data for any other purpose, or (2) opting the individual out of the processing of that personal data for any purpose except for those exempted under the law.[35] In contrast, Delaware and New Jersey require the controller to delete the data in question rather than merely opt the individual out of non-exempt processing.[36]

---

[31] *E.g.*, Colo. Rev. Stat. § 6-1-1307(3) (2023); Conn. Gen. Stat. § 42-523(d) (2023). For the typical definition of pseudonymous data, see *supra* fn. 23 and accompanying text.
[32] Tenn. Code. Ann. § 47-18-3207(d) (2024); 2024 R.I. Pub. Laws ch. 430, § 6-48.1-7(n).
[33] *Policy Principles for a Federal Data Privacy Framework in the United State: Hearing Before the S. Comm. on Commerce, Science, & Transportation*, 116th Cong. 3 (2019) (testimony of Woodrow Hartzog, Prof. Northeastern University).
[34] *See generally* Samuel Adams & Stacey Gray, *Survey of Current Universal Opt-out Mechanisms*, FPF (Oct. 12, 2023), https://fpf.org/blog/survey-of-current-universal-opt-out-mechanisms.
[35] These provisions are designed to solve for a situation in which a controller acquires personal data from a data broker, responds to a deletion request from an individual, then reacquires the data from a data broker.
[36] Del. Code. Ann. tit. 6, § 12D-104(c)(5) (2024); N.J. Stat. Rev. § 56:8-166.10 (2024).

4. Business Obligations

In addition to responding to individual rights requests, organizations subject to these laws face a number of obligations that do not require action by individuals, such as:

- **Transparency:** Controllers are required to be transparent by providing a "reasonably accessible, clear and meaningful privacy notice" that includes information such as categories of personal data processed, processing purposes, how to exercise individual rights and appeal decisions, categories of personal data shared with third parties, and contact information.[37]
- **Data Minimization & Purpose Limitation:** Controllers must typically limit the ***collection*** of personal data to what is "adequate, relevant, and reasonably necessary" for the purposes disclosed to the individual.[38] Controllers must obtain opt-in consent to ***process*** personal data for purposes that are "neither reasonably necessary to, nor compatible with the disclosed purposes for which such personal data is processed."[39] Utah, Iowa, and Rhode Island are notable outliers for not having these data minimization or purpose limitation requirements,[40] whereas Maryland has introduced novel requirements that tie the collection and use of personal data to what is necessary to provide or maintain a requested product or service.[41]
- **Data Security:** Controllers must maintain "reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data." In 2024, Minnesota became the first state to explicitly require controllers to maintain an "inventory of the data" as part of those data security responsibilities.[42]
- **Processor Agreements:** Controllers must engage in oversight of processors by entering into a contract that meets a set of statutory criteria, which typically include: setting forth instructions for processing the personal data, the nature and purpose of the processing, types of data subject to processing, duration of processing, and each parties' rights and obligations; binding the processor to a duty of confidentiality; specifying whether the personal data should be deleted or returned when the processor ceases to provide services; placing restrictions on a processor's ability to engage a subcontractor;[43] and

---

[37] *E.g.*, Conn. Gen. Stat. § 42-520 (2023).
[38] *Id.*
[39] *Id.*
[40] Others have argued that these are implicit requirements of those laws. Centre for Information Policy Leadership, *Data Minimization in the United States' Emerging Privacy Landscape: Comparative Analysis and Exploration of Potential Effects* (Aug. 2024), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_data_minimization_us_privacy_landscape_aug24.pdf.
[41] *Infra* Part II.C.
[42] 2024 Minn. Laws Ch. 121, https://www.revisor.mn.gov/laws/2024/0/Session+Law/Chapter/121.
[43] While each of the 19 states covered by this report require a processor to bind a subcontractor with an agreement that imposes all of the law's processor obligations, seven of the nineteen state laws—Colorado, Connecticut, Delaware, Maryland, Minnesota, New Hampshire, and Rhode Island—provide that a processor must first provide the controller with an opportunity to object before the processor may engage that subcontractor. The CCPA, in contrast, requires a service provider to provide notice to a business if it engages another person to assist it in processing personal information for a business purpose. Cal. Civ. Code § 1798.140, subd. (ag)(2).

obligating the processor to cooperate with assessments by the controller to determine the processor's compliance with the law.

- **Anti-discrimination:** Controllers are typically barred from processing personal data in violation of state and federal laws prohibiting unlawful discrimination.[44] Maryland has taken a slightly different approach to anti-discrimination obligations, inspired by a 2022 federal bill, the American Data Privacy and Protection Act (ADPPA). Maryland's law includes the typical prohibition on processing personal data in violation of state and federal laws prohibiting unlawful discrimination. Maryland's law, however, additionally prohibits controllers from collecting, processing, or transferring personal data ***or publicly available data***—a unique requirement—in a manner that "unlawfully discriminates in or otherwise unlawfully makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity, or disability," subject to limited exceptions (including self-testing to prevent or mitigate unlawful discrimination and diversifying an applicant or customer pool). This provision could be stronger than other laws' anti-discrimination provisions because it applies to processing of "publicly available data,"[45] but it might be undercut by the focus on "unlawful discrimination," which is potentially a higher threshold than other potential standards, such as all discrimination or unjustified differential treatment.
- **Non-retaliation:** Controllers are prohibited from retaliating against an individual—by denying goods or services, increasing prices, or degrading the product or service—for exercising their rights. That restriction is typically paired with an exception providing that it shall not be construed to (1) require a controller to provide or service if doing so requires personal data that the controller does not collect or maintain, or (2) charge a different price, rate, level, quality, or selection of goods or services to an individual if that offering is made in connection with an individual's participation in a bona fide loyalty program or similar rewards system.[46]
- **Data Protection Assessments:** For processing activities that present a heightened risk of harm, controllers must conduct and document a data protection assessment (DPA). Processing activities that require a DPA include, but are not limited to: Processing personal data for targeted advertising; selling personal data; processing sensitive data; and profiling that presents a reasonably foreseeable risk of substantial injury to individuals, such as unlawful disparate impact, financial injury, or intrusion upon seclusion which would be offensive to a reasonable person.[47] At a high-level, comprehensive privacy laws require DPAs to include a balancing test: Compare benefits that flow from the

[44] Minnesota's law included a more detailed different formulation of its antidiscrimination requirement, prohibiting controllers from processing an individual's or a class of individuals' personal data on the basis of their "actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income, or disability in a manner that unlawfully discriminates against the [individual or class of individuals] with respect to the offering or provision of: housing, employment, credit, or education; or the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation." 2024 Minn. Laws Ch. 121.
[45] This term is undefined, but it could be synonymous with the defined term "publicly available information."
[46] *E.g.*, Conn. Gen. Stat. § 42-520(b) (2023); Va. Code Ann. § 59.1-578(A)(4) (2023).
[47] *E.g.*, Conn. Gen. Stat. § 42-522 (2023).

processing activity (to the controller, the individual, and other stakeholders) against risks posed to the individual as mitigated by safeguards employed by the controller.[48]

5. Enforcement

The enforcement provisions in laws based on the WPA framework tend to follow the same basic structure. Enforcement authority is typically vested exclusively with the attorney general and violations of the law are typically treated as violations of the state's Unfair and Deceptive Acts and Practices (UDAP) law, with penalties rising up to $7,500 per violation in most states.[49]

These comprehensive privacy laws also typically include a cure provision, providing that, before bringing suit, the attorney general must provide notice of alleged violations to a controller and grant that controller a certain amount of time (e.g., sixty days) to "cure" any alleged violations of the law. After that cure period expires, the attorney general can only bring suit if the controller failed to cure the violation or made misrepresentations to the attorney general. Cure periods fall into one of several categories based on (1) whether the cure notice is mandatory or permissive from the attorney general's perspective, and (2) whether the cure period "sunsets" after a set date. Some cure periods are mandatory in that the attorney general must always provide an opportunity to cure. Some cure periods are "mandatory where possible," meaning that the attorney general must provide an opportunity to cure but only if they deem that a cure is "possible." For laws with mandatory and "mandatory where possible" cure provisions, there is a split as to whether the cure provision sunsets, meaning that, on a set date (e.g., two years after the law's effective date), the attorney general is no longer required to offer controllers the chance to cure alleged violations of the law before bringing an enforcement action for said violation.

Cure Provision	States
Mandatory - No Expiration Date	Indiana, Iowa, Kentucky, Nebraska, Tennessee, Texas, Utah, Virginia
Mandatory - Expiration Date	Minnesota, Montana
Mandatory (If Possible) - Expiration Date	Colorado, New Jersey, Oregon, Connecticut, Delaware, New Hampshire
Permissive / None	California, Maryland, Rhode Island

Table 3. Categorization of Cure Provisions

[48] *Id.*
[49] *E.g.*, Va. Code Ann. § § 59.1-584 (2023). Every state has some form of UDAP law. *Consumer Protection Laws: 50-State Survey*, JUSTIA (Oct. 2023), https://www.justia.com/consumer/consumer-protection-laws-50-state-survey.

Another common aspect of the enforcement provisions is that laws adhering to the WPA framework typically disclaim that nothing in the act shall be construed as providing the basis for, or be subject to, a private right of action for violations of that act ***or under any other law***.

PRA Confusion in New Jersey: When New Jersey's law was enacted in January 2024, industry groups critiqued the law for reintroducing uncertainty around private right of action because the bill had been amended to drop the "or under any other law" language seen in many other state laws.[50] Instead, New Jersey's law provides that "[n]othing in [the law] shall be construed as providing the basis for, or subject to, a private right of action for violations of [the law]."[51] In his signing statement, Governor Murphy attempted to assuage those industry fears by arguing that "nothing in this bill expressly establishes such a private right of action" and "this bill does not create a private right of action under this law or under any other law."[52]

C. The California Consumer Privacy Act

California was the first state to enact a comprehensive privacy law. Despite this, no other state has enacted a law relying on the California Consumer Privacy Act (CCPA) as its model. Rather, some states have incorporated elements of the CCPA into the WPA framework, such as a broad definition of sale.[53] While the structure and terminology of the CCPA is different from the WPA framework, many of the core roles, obligations, and rights are similar, as both were inspired to various degrees by the European Union's General Data Protection Regulation (GDPR). Nevertheless, the CCPA is longer, more complex, and subject to a growing body of regulations, further distinguishing it from laws based on the WPA framework. The following subsections briefly cover the scope and core rights and obligations of the CCPA, with an emphasis on differences from the WPA framework.

1. Covered Entities

The CCPA primarily applies to ***"businesses,"*** a category analogous to controllers under the WPA framework. Businesses include legal entities operating for profit or financial benefit that collect individuals' personal information or determine the purpose and means of processing individuals' personal information and either (A) had annual gross revenue exceeding $25 million in the preceding year, (B) buys, sells, or shares the personal information of 100,000 or more individuals or households, or (C) derives 50% or more of annual revenue from selling or sharing individuals' personal information.[54] The second most important role in the CCPA is that of ***service providers***. Conceptually similar to processors under the WPA framework, service providers are persons that process personal information on behalf of a business for a "business purpose" pursuant to a

[50] N.J. Bus. & Indus. Ass'n, *NJBIA Calls for Legislative Cleanup of New Data Privacy Law*, NJBIA (Jan. 17, 2024), https://njbia.org/njbia-calls-for-legislative-cleanup-of-new-data-privacy-law.
[51] N.J. Stat. Rev. § 56:8-166.19 (2024).
[52] Press Release, Off. Gov. Phil Murphy, Governor's Statement upon Signing Senate Bill No. 332 (Sixth Reprint) (Jan. 16, 2024), https://d31hzlhk6di2h5.cloudfront.net/20240116/da/1f/46/be/fa0e699395c8e1426fe07349/S332_.pdf.
[53] *See supra* fn. 14 and accompanying text.
[54] Cal. Civ. Code § 1798.140, subd. (d)(1). There are additional rules by which a person, entity, or joint venture or partnership could be considered a business.

written contract prohibiting the service provider from taking certain actions such as selling or sharing the personal information or using it for any purpose other than the specified business purpose. ***Business purpose*** is a defined set of operational activities, including auditing for ad impressions, ensuring security and integrity, debugging, performing services on behalf of a business, and more.[55]

While the CCPA terms "business" and "service provider" are somewhat comparable to controllers and processors under the WPA framework, the CCPA includes additional roles that trigger unique obligations: contractors and third parties. ***Contractors*** are persons to whom the business makes personal information available for a "business purpose." Like service providers, contractors must receive personal information pursuant to a written contract that prohibits the contractor from certain actions, such as selling/sharing personal information or using personal information for purposes other than those specified in the contract. ***Third parties*** are everyone else—persons who are not the business with whom an individual intentionally interacts, a service provider to the business, or a contractor. Certain rights and obligations are triggered by interactions with third parties. For example, sale of personal information to a third party triggers contractual and oversight obligations by a business.

2. Covered Data

The CCPA covers the collection and use of ***personal information*** and ***sensitive personal information***. Although analogous to "personal data" under the WPA framework, the term "personal information" is more detailed under CCPA. 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."[56] In contrast to the WPA framework, the CCPA applies to ***employee*** and ***business-to-business (B2B) data***.[57] Given that broader scope of covered data, the CCPA is arguably the most "comprehensive" of the state comprehensive privacy laws. The definition also includes a long, illustrative list of categories of personal information, such as identifiers, characteristics of protected classifications, commercial information (e.g., purchase history), biometric information, olfactory information, inferences drawn from any of the information identified in the definition, sensitive personal information, and more.[58] In 2024, the CCPA was amended to clarify that personal information can exist in various formats, including physical formats (e.g., "paper documents, printed images, vinyl records, or video tapes"), digital formats (e.g., "text, image, audio, or video files"), and abstract digital formats (e.g., "compressed or encrypted files, metadata, or artificial intelligence systems that are capable of outputting personal information").[59] Similar to WPA laws, personal information does not include publicly available information or information that is deidentified or "aggregate consumer information," however, unlike most WPA laws, the CCPA does not include carve outs for "pseudonymous" information.

---

[55] *Id.* subd. (e).
[56] Cal. Civ. Code § 1798.140, subd. (v).
[57] Brian Hengesbaugh & Cristina Messerschmidt, *CCPA/CPRA Grace Period for HR and B2B Ends Jan. 1*, IAPP (Sept. 7, 2022), https://iapp.org/news/a/ccpa-cpra-grace-period-for-hr-and-b2b-ends-jan-1.
[58] *Id.*
[59] A.B. 1008, 2024 Reg. Sess., (Cal. 2024).

The CCPA also designates certain types of information as sensitive, subject to heightened protections and obligations. Sensitive personal information includes: Personal information that reveals certain identifiers (e.g., social security number), certain financial information (e.g., account log-in), precise geolocation (scoped at 1,850 feet), certain sensitive characteristics (e.g., racial or ethnic origin), the contents of certain communications (e.g., email), an individual's genetic data, or an individual's neural data; biometric information processed for uniquely identifying an individual; "personal information collected and analyzed concerning a consumer's health"; and "personal information collected and analyzed concerning a consumer's sex life or sexual orientation."[60] The California Privacy Protection Agency has authority to adopt regulations updating or adding categories of sensitive personal information.[61]

3. Individual Rights

The CCPA endows rights that are largely similar to those under the WPA framework, including to know what personal information is being collected and access that information, correct inaccurate personal information, delete the personal information that was collected directly from them,[62] to know what personal information is sold or shared and to whom, to opt-out of the sale or sharing of personal information, and to limit the use and disclosure of sensitive personal information. The obligations and rights concerning sensitive personal information is a key difference between the CCPA and the WPA framework. Whereas laws adhering to the WPA framework typically require opt-in consent for processing sensitive data, the CCPA takes an opt-out approach whereby individuals can direct a business to limit its use of sensitive personal information "to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services," to perform certain "business purposes" under the statute, and as authorized in the regulations.[63]

Another notable difference between the CCPA and the WPA framework with respect to individual rights is the role of authorized agents. Under the WPA framework, an authorized agent typically can only exercise opt-out rights on behalf of an individual. Under CCPA, however, individuals may use authorized agents to submit other rights requests on their behalf, including for opt-out of sale/share, limiting unnecessary processing of sensitive personal information, deleting personal information, correcting personal information, or to know what personal information is sold or

[60] Cal. Civ. Code § 1798.140, subd. (ae); S.B. 1223, 2024 Reg. Sess., (Cal. 2024).
[61] Cal. Civ. Code § 1798.185, subd. (a)(1).
[62] Unlike the WPA framework, which extends deletion rights to data collected from third parties. At the time of writing, the CPPA is considering adopting changes to the CCPA regulations to include requirements that a business must ensure "implement measures to ensure that the information remains deleted," and provides, as an example, that "if a business . . . receives personal information about consumers from data brokers on a regular basis, failing to consider and address how deleted information may be re-collected by the business factors into whether that business, service provider, or contractor has adequately complied with a consumer's request to delete." Cal. Priv. Prot. Agency, Proposed Text of Regulations (October 2024), https://cppa.ca.gov/meetings/materials/20241004_item3_draft_text.pdf.
[63] Cal. Civ. Code § 1798.121, subd. (a). *But see id.* subd. (d) ("Sensitive personal information that is collected or processed *without the purpose of inferring characteristics about a consumer* is not subject to this section . . . and shall be treated as personal information for purposes of all other sections of this act, including Section 1798.100.") (emphasis added).

shared.[64] Allowing authorized agents to exercise a greater number of rights on an individual's behalf could have the benefit of reducing friction and costs for individuals to exercise all of their rights under the law. On the other hand, the increased role of authorized agents also poses risks to individuals, as businesses have to guard against fraudulent authorized agent requests that could, for example, give a bad actor access to an individual's personal information.

4. Business Obligations

Business obligations under the CCPA also roughly resemble those under the WPA framework, although there are some important differences in the details and the CCPA has additional obligations. At a high level, businesses must adhere to the following:

- **Transparency:** Businesses subject to the CCPA are required to provide a privacy policy, which is similar to the privacy notice under the WPA framework, and a "Notice at Collection" that, at or before the time of collection, informs individuals as to the categories of personal information collected, the purposes for which those categories of personal information are collected, and whether that information is sold/shared.[65] Businesses also must disclose how long they intend to retain each category of personal information and sensitive personal information or the criteria for determining how long it shall hold such information.[66]
- **Data Minimization and Purpose Limitation:** Businesses cannot collect additional categories of personal information or sensitive personal information, nor use such information previously collected for additional purposes incompatible with the disclosed purpose at collection, without providing new notice to the individual. The law's implementing regulations go further, limiting the collection and processing of personal information to what is reasonably necessary and proportionate to achieve a disclosed purpose that is consistent with a person's ***reasonable expectations***, another disclosed purpose that is compatible with the context in which the personal information was collected, or another disclosed purpose for which the business obtained consent.[67]
- **Data Security:** Businesses must implement "reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with [Cal. Civ. Code] Section 1798.81.5."[68] The CCPA directs the California Privacy Protection Agency to issue regulations requiring businesses whose processing of individuals' personal information presents significant risk to individuals' security to perform an annual cybersecurity audit.
- **Oversight:** Businesses must enter into contracts and engage in oversight of certain other entities with whom they interact. If a business ***sells/shares*** personal information with a

[64] Cal. Civ. Code § 1798.130, subd. (3); Cal. Code Reg. tit. 11, § 7026, subd. (j) (2023); *Id.* § 7027, subd. (j); *Id.* § 7063.
[65] Cal. Civ. Code § 1798.100, subd. (a)(1). If the business collects sensitive personal information, it must make the same disclosure specific to categories of sensitive personal information. *Id.* subd. (a)(2).
[66] *Id.* subd. (a)(3). For more on transparency requirements under the CCPA, see California Privacy Protection Agency, *What General Notices Are Required By The CCPA?*, https://cppa.ca.gov/pdf/general_notices.pdf.
[67] Cal. Code Reg. tit. 11, § 7002 (2023).
[68] Cal. Civ. Code § 1798.100, subd. (e).

third party or ***discloses*** it to a service provider or contractor for a business purpose, it must enter into an agreement that specifies that the information is sold/shared/disclosed only for "limited and specified purposes," obligates the recipient to comply with applicable obligations under the CCPA and to provide the same level of privacy protection as required under the law, allowing the business "to take reasonable and appropriate steps" to ensure that the recipient uses the information "in a manner consistent with the business' obligations" under the CCPA, requiring the recipient to notify the business if it can no longer meet its obligations under the CCPA and then granting the business the right "to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information."[69]

- **Non-retaliation:** Businesses may not discriminate against an individual for exercising a right under the CCPA, ***but*** businesses may offer financial incentives for the collection, sale/sharing, or retention of personal information and may charge a different price or provide a different quality of goods or service where the difference in price or quality is reasonably related to the value provided to the business by the personal information.[70]

Ongoing Rulemaking: The CCPA is unique amongst the state comprehensive privacy laws for having a standalone agency (the CPPA) tasked with enforcement and rulemaking. Prior to the CPRA's enactment, the California Attorney General (AG) had rulemaking authority under the CCPA, and the AG's office finalized a set of initial regulations in 2020.[71] The CPRA transferred rulemaking authority to the CPPA, and the agency finalized its first set of regulations in March 2023. As of July 2024, the CPPA is considering additional rulemaking packages relating to data brokers (pursuant to the DELETE Act of 2023),[72] cybersecurity audits,[73] risk assessments, automated decisionmaking technology, and updates to existing regulations.

[69] *Id.* subd. (d).
[70] Cal. Civ. Code § 1798.125.
[71] Press Release, Cal. Off. Att'y Gen., *Attorney General Becerra Announces Approval of Final Regulations Under the California Consumer Privacy Act* (Aug. 14, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-final-regulations-under-california.
[72] Cal. Civ. Code § 1798.99.80 *et seq.* Enacted in 2023, the DELETE Act directed the CPPA to establish a bulk deletion mechanism linked to the California data broker registry, allowing Californians to submit a single request to require that their personal data be deleted from the databases of the registered data brokers, subject to limited exceptions.
[73] Requiring businesses to conduct cybersecurity audits will be a novel business obligation which is not present in any of the WPA framework variants.

II. Recent Legislative Developments and Trends

The state privacy law landscape proves true the old adage that the states are laboratories of democracies. Six years on from the CCPA's enactment, newly enacted laws iterate on existing frameworks, and trends are emerging: states are adjusting applicability thresholds; the scope of sensitive data is expanding; substantive data minimization requirements are emerging; consumer health data and adolescents' data are receiving unique protections; and new individual rights, like the ability to contest (not merely opt-out of) adverse profiling decisions, are being established.

A. States Tinkering with Applicability Thresholds

States have been experimenting with scope and applicability thresholds in a variety of ways, including changes to numerical thresholds, a novel small business exemption, and fewer entity-level exemptions for organizations subject to existing federal privacy laws.

Crunching the Numbers. Laws based on the WPA framework typically have two-tiers of applicability thresholds for the number of in-state residents' whose personal data are processed. There is a default threshold (e.g., 100,000) and a second, lower threshold (e.g., 25,000) which is connected to a revenue requirement (e.g., 20%) from selling personal data ("default threshold" and "data brokerage threshold," respectively). Montana was the first state to lower the default threshold (to 50,000) in 2023, and Delaware later lowered that threshold again (to 35,000).

These lowering default thresholds, particularly in states with low population numbers, raise a question as to whether the applicability thresholds are rising, falling, or remaining constant as a proportion of a state's population—i.e., are thresholds of 100,000 Virginians, 50,000 Montanans, and 35,000 Delawareans equivalent? Table 4 (Appendix) includes data on state populations, default and data brokerage applicability thresholds from relevant laws, and those thresholds as a percentage of the state's population. Those percentages are plotted in Figure 2 below, ordered chronologically by enactment date. Ordering states' applicability thresholds by the date on which each state law was enacted shows how these thresholds are changing over time and whether there is a trend towards higher or lower thresholds.

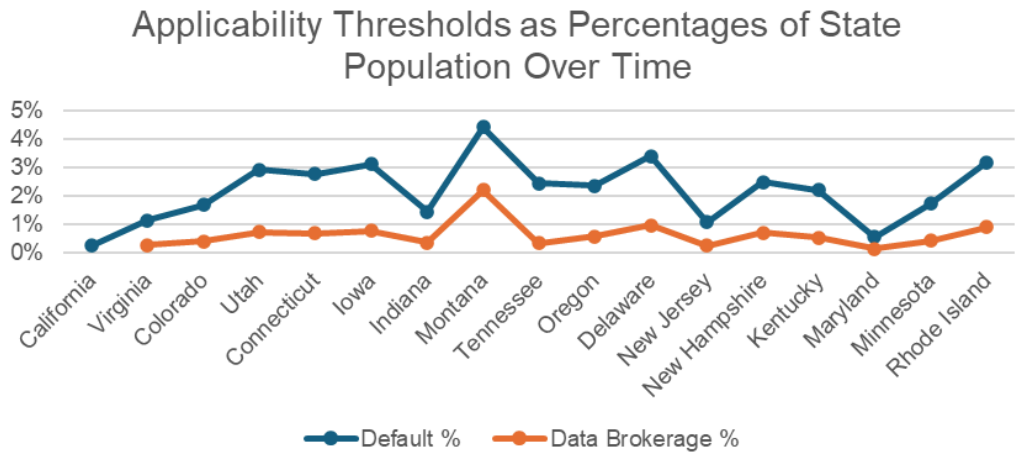

Figure 2. Applicability Thresholds as Percentages of State Population

These data reveal a few insights into whether and how scope is changing over time. The numerical cut-offs of 100,000 or 25,000 affected individuals proved relatively sticky for a number of years. Once Delaware lowered those thresholds to 35,000 and 10,000, several states followed suit. Those thresholds, however, are not drastically lower than prior thresholds as a percentage of population. Notable outlier states include Montana, which has the highest percentage thresholds, and California, New Jersey, and Maryland, which have relatively low thresholds. The data brokerage thresholds are holding relatively steady under 1% of the state's population, with the exception of Montana. For data on controller applicability thresholds, see Table 4 (Appendix).

Small Businesses. In 2023, Texas became the first state to eschew numerical thresholds in its comprehensive privacy law; rather, the law applies to any person that (1) conducts business in Texas or produces a product or service consumed by Texas residents, (2) processes or sells personal data; and (3) is not a small business as defined by the United States Small Business Administration (USSBA).[74] Nebraska became the second state after Texas to forgo the numerical applicability thresholds in favor of an exemption for small businesses as defined by the USSBA. Minnesota hybridizes these approaches, including numerical thresholds and the Texas- and Nebraska-style small business exemption. These states are marked with an asterisk in Table 4 (Appendix). Under Texas's approach, small businesses are still prohibited from selling sensitive data without obtaining consent from the affected individuals.[75] In that way, Texas's approach is arguably stronger than other laws which wholly exempt any organizations that do not meet the processing or data brokerage thresholds to be a "controller."

Texas defected from the numerical threshold standard in favor of this small business exception due to pushback from stakeholders that numerical thresholds are arbitrary and that revenue requirements are uncertain, whereas the USSBA small business exception is intended to be clearer, tailored to different industries, and not entail additional compliance costs to determine whether an organization is within scope.[76]

Preference for Data-level Exemptions. States are also experimenting with including fewer entity-level exemptions in favor of data-level exemptions, only carving out the specific data subject to an existing federal law rather than the entire entity that holds such information:

Gramm-Leach Bliley (GLBA): Sixteen of the nineteen state comprehensive privacy laws have entity-level exemptions for financial institutions that are subject to Title V of the GLBA.[77] In 2023 and 2024, Oregon and Minnesota became the second and third states to include only a data-level exemption for GLBA,

[74] Tex. Bus. & Com. Code § 541.002(a) (2024). The definition of a "small business" under USSBA regulations varies by industry. *See* 13 C.F.R. part 121. Typically, having fewer than 500 employees qualifies as a "small business." Off. of Advocacy, U.S. Small Business Admin., *Frequently Asked Questions*, (Mar. 2023), https://advocacy.sba.gov/wp-content/uploads/2023/03/Frequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf.

[75] Tex. Bus. & Com. Code § 541.107 (2024).

[76] Memorandum from the Off. of Texas Representative Giovanni Capriglione on "Texas vs. Virginia Consumer Data Protection Act Comparison" (Jan. 24, 2023) (on file with author).

[77] Many of these state laws with entity-level GLBA exemptions also include data-level exemptions for data subject to Title V.

after California. This emerging trend away from entity-level exemptions for financial institutions stems in part from concerns that entities are availing themselves of the GLBA exemption in situations which were not intended, such as car dealerships that have a financing wing claiming that their entire business is exempt under the law.[78] Echoing similar concerns, in February 2024, Connecticut Attorney General Tong released a report detailing the first six months of enforcement under the Connecticut Data Privacy Act and recommending scaling back the entity-level exemptions in that law.[79] The states that have forgone a GLBA entity-level exemption have included exemptions for traditional financial bodies such as banks, financial institutions, and insurers as defined under state law.[80]

Health Insurance Portability and Accountability Act (HIPAA): The trend away from entity-level exemptions is more pronounced for HIPAA. Only two of the first ten state comprehensive privacy laws to be enacted did not include entity-level HIPAA exemptions, whereas six of the last nine enacted laws include only data-level HIPAA exemptions. That trend is likely a response to the U.S. Supreme Court's 2022 decision in *Dobbs v. Jackson Women's Health Organization* overturning *Roe v. Wade* and the resultant heightened public concern over health privacy and criminalization of reproductive healthcare services.

Family Educational Rights and Privacy Act (FERPA): Seventeen of the nineteen state comprehensive privacy laws exempt personal data regulated by FERPA. In 2024, New Jersey became the second state, after California, not to include a data-level exemption for FERPA.

Nonprofits & Institutions of Higher Education: Thirteen of the nineteen state comprehensive privacy laws include broad exemptions for nonprofits. However, five of the last nine of those laws enacted did not include a general nonprofit exemption, instead including narrow entity- or data-level exemptions for select nonprofits, such as those assisting first responders in responding to catastrophic events. Similarly, five of the last nine enacted laws did not include exemptions for institutions of higher education, although Minnesota's law included a delayed effective date for postsecondary institutions.

B. Expanding Scope of Sensitive Data

The U.S. regulatory discussion around data privacy has long assumed that some categories of personal data—like race, religion, and health information—are more sensitive than others in that collection and use of that information is more likely to present a heightened risk of harm to someone, especially if misused or breached.[81] Thus, lawmakers have attempted to define categories of sensitive data which are subject to heightened protections under the law.[82]

---

[78] *See, e.g.*, *Hearing on S.B. 619 Before the S. Comm. on Judiciary*, 2023 Reg. Sess. (Or. Mar. 7, 2023) https://olis.oregonlegislature.gov/liz/2023R1/Downloads/PublicTestimonyDocument/59865 (testimony of Kimberly McCullough, Legislative Director, Oregon Department of Justice).
[79] Off. Att'y Gen. Conn., Report to the General Assembly's General Law Committee Pursuant to Public Act 22-15, "An Act Concerning Personal Data Privacy and Online Monitoring," Referred to As the "Connecticut Data Privacy Act" ("CTDPA") Codified as Conn. Gen. Stat. § 42-515 et seq. at 7 (Feb. 2024), https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf.
[80] *E.g.*, Or. Rev. Stat. § 646A.572(2)(L), (n) (2023); 2024 Minn. Laws Ch. 121, § 325O.03, subd. (2)(a)(16), (18) https://www.revisor.mn.gov/laws/2024/0/Session+Law/Chapter/121.
[81] Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. L. REV. 1081, 1088–99 (2024).
[82] For sensitive data obligations, see *supra* Parts I.B.3 & I.C.3.

As the number of states with comprehensive privacy laws expands, so too has the scope of sensitive data as states add to or iterate upon existing definitions. Table 5 (Appendix) compiles the various subsets of sensitive data across the nineteen comprehensive state privacy laws to show how fractured and expansive the notion of sensitive data has become. Comparable elements, such as the myriad different articulations of health data, are grouped together for ease of comparison. Some notable trends have emerged: Lawmakers have tinkered with the definitions of health data, expanding coverage beyond diagnosis to cover conditions and treatments; states have added a new category of "status as victim of a crime"; Colorado and California have amended their laws to add neural data; four states now consider data revealing status as transgender or non-binary to be sensitive; and several states have expanded the definition of biometric data to include certain data that *can* be used for identification purposes, not just data that are used for such purposes.

C. Data Minimization: Moving from Procedural Rules to Substantive Standards

Data minimization is rooted in the earliest instances of U.S. privacy law, going all the way back to the original Fair Information Practices and the Privacy Act of 1974.[83] Data minimization has emerged as a priority issue in recent years as many privacy advocates have actively encouraged a shift in U.S. privacy law away from the maligned notice-and-choice model.[84] As discussed above, the majority of state comprehensive privacy laws include a procedural data minimization rule that limits collection and processing of personal data to what is "adequate, relevant, and reasonably necessary" to achieve the purposes that are ***disclosed*** to an individual, and any unnecessary or incompatible secondary uses of personal data require opt-in consent. This is a procedural rule because it is agnostic as to the substantive processing purpose. Rather, whether collection and processing can occur turns on procedural requirements of disclosure and consent.

Maryland broke this trend by including a novel rule that tied collection of personal data (and the collection, processing, and sharing of sensitive data) to whether that data is reasonably (or strictly) ***necessary to provide or maintain*** a requested product or service. Maryland's provisions are substantive data minimization rules because whether collection can occur turns on the nature of the processing activity. The table below contrasts the two regimes:

	Procedural Data Minimization (pre-2024)	Substantive Data Minimization (NEW)
Collecting Personal Data	A controller must limit 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 the individual***.	Controllers must limit the ***collection*** of personal data to what is ***reasonably necessary and proportionate to provide or maintain a specific product or service*** requested by the individual.

[83] Robert Gellman, *Fair Information Practices: A Basic History*, BOB GELLMAN (Apr. 9, 2024), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[84] For more on this legislative shift, see Jordan Francis, *Unpacking the Shift Toward Substantive Data Minimization Rules in Proposed Legislation*, IAPP (May 22, 2024), https://iapp.org/news/a/unpacking-the-shift-towards-substantive-data-minimization-rules-in-proposed-legislation.

	Procedural Data Minimization (pre-2024)	Substantive Data Minimization (NEW)
Processing Personal Data & Secondary Use	Unless the controller obtains the individual's ***consent***, a controller may not process personal data for ***purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes*** for which such personal data is processed.	Unless the controller obtains the individual's ***consent***, a controller may not process personal data for ***purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes*** for which such personal data is processed.
Processing Sensitive Data	Processing ***sensitive data*** requires opt-in, affirmative ***consent***.	Controllers may not ***collect, process, or share sensitive data*** unless the collection or processing is ***strictly necessary to provide or maintain a specific product or service*** requested by the individual. Controllers are ***prohibited*** from ***selling*** sensitive data.

Table 6. Data Minimization Standards

Maryland's law is not yet in effect and it is unclear as of yet what the impact of its language will be. There are significant unresolved questions, including the scope of what is "necessary" to provide or maintain a product or service (i.e., whether a business can define selling personal data to be necessary to offering their service), the difference between "reasonably necessary" and "strictly necessary," and whether obtaining consent can override the substantive rules.

The California Privacy Protection Agency (CPPA) has pioneered a "hybrid" approach. Finalized in 2023, the law's implementing regulations provide that collection and processing of personal information must be limited to what is reasonably necessary and proportionate to achieve either: a disclosed purpose that is consistent with a person's ***reasonable expectations***, another disclosed purpose that is compatible with the context in which the personal information was collected, or another disclosed purpose for which the business obtained the individual's consent. Factors for whether collection or processing is consistent with an individual's reasonable expectations include:

- "The relationship between the consumer(s) and the business";
- "The type, nature, and amount of personal information that the business seeks to collect or process";
- "The source of the personal information and the business's method for collecting or processing it;"
- "The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing materials to the consumer(s) about the business's good or service"; and

- "The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s)."[85]

Thus, under California's rule, disclosures made by the business are a relevant but not dispositive factor in the test for whether a processing purpose is consistent with an individual's reasonable expectations. This rule can be thought of as a hybrid rule because it still relies on procedural factors (e.g., disclosures made) but it also incorporates substantive factors about the relationship between the parties. For sensitive data, California allows individuals to opt-out of unnecessary processing, but only if the sensitive data is collected or processed for the purpose of inferring characteristics about the individual.

D. Heightened Protections for Certain Types of Data: Adolescents, Health, and Biometrics

Privacy risks around health data, adolescents' data, and biometrics have been at the forefront of policy debates in recent years. This broad public awareness has led to sectoral bills, such as Washington's My Health My Data Act or the Age-Appropriate Design Codes enacted in California and Maryland, but it has also manifested as new and enhanced health-, youth-, and biometrics-specific provisions in comprehensive privacy legislation.

1. Adolescent Privacy Amendments and Trends

The Children's Online Privacy Protection Act (COPPA) has been federal law since 1998,[86] and state comprehensive privacy laws typically regard personal data concerning a known child as sensitive data subject to the COPPA Rule's consent requirements. In recent years, state laws have been expanding their youth privacy protections to include heightened protections for teenagers as well. These changes fall into two different categories: making opt-out rights opt-in requirements with respect to teenagers, and, less commonly, enacting large, structural changes to the law to add heightened protections such as a duty of care and additional impact assessment requirements with respect to children' and teens' data.

Opt-ins: Following California's lead,[87] several states have recently created opt-in requirements with respect to processing teens' personal data for certain purposes. The scope of these requirements vary between states in two ways—which activities require opt-in consent and what age ranges are covered. For example, New Jersey has the broadest scope in terms of covered activities: Controllers must obtain opt-in consent for (i) targeted advertising, (ii) sale of personal data, or (iii) profiling in furtherance of legal or similarly significant decisions for individuals the controller knows or wilfully disregards are older than 13 but younger than 17. Delaware has narrower scope in terms of covered activities (applying only to targeted advertising and sale of

[85] Cal. Code Reg., tit. 11, § 7002(b) (2023).
[86] 15 U.S.C. § 6501 *et seq.*
[87] The CCPA's right to opt-out of sale of personal information includes a provision prohibiting businesses from selling individuals' personal information if the business has actual knowledge that the individual is less than 16 years of age, but allowing opt-in consent to such sale (by a parent or guardian for an individual under 13 or by the individual themself if they are older than 13 but younger than 16).

personal data) but it has the broadest scope of ages covered (older than 13 but younger than 18). States like New Hampshire and Minnesota have heightened protections that are narrower than those in New Jersey and Delaware, requiring controllers to obtain opt-in consent for (i) targeted advertising or (ii) sale of personal data for individuals the controller knows or wilfully disregards are older than 13 but younger than 15. Teens' (aged 13 and older) consent[88] is required for the following activities at the following age ranges:

State	Protected Ages	Sale	Targeted Advertising	Profiling
California	Under 16	X	X	
Connecticut	Under 16	X	X	
Montana	Under 16	X	X	
Oregon	Under 16	X	X	X
Delaware	Under 18	X	X	
New Jersey	Under 17	X	X	X
New Hampshire	Under 16	X	X	
Minnesota	Under 17	X	X	

Table 7. Teenager Opt-in Requirements

Rather than imposing opt-in requirements, Maryland has gone further than other states by prohibiting targeted advertising and the sale of personal data if the controller knew or should have known that the individual was under the age of 18.[89]

New Rights and Obligations: In 2023, Connecticut passed SB 3, a bill which amended the Connecticut Data Privacy Act (CTDPA) to add significant new protections for adolescent data.[90]

[88] For Connecticut, New Hampshire, and Delaware, there is some ambiguity as to whether the consent requirement applies only to the sale of personal data, in which case the restriction on targeted advertising to teens would operate as a prohibition. The Delaware attorney general interprets the consent requirement as applying to both. Delaware Dep't of Justice, *Frequently Asked Questions*, https://attorneygeneral.delaware.gov/fraud/personal-data-privacy-portal/frequently-asked-questions ("[T]he DPDP Act requires controllers to obtain opt-in consent before selling a consumer's personal data, or processing personal data for the purposes of targeted advertising, when the consumer is under 18 years old).

[89] This "or should have known" language is different from the "willfully disregards" knowledge standard used in many other state comprehensive privacy laws, and it could imply a requirement to engage in age-estimation or age-gating. David Stauss, *Maryland Legislature Passes Consumer Data Privacy Bill*, LinkedIn (Apr. 7, 2024), https://www.linkedin.com/pulse/maryland-legislature-passes-consumer-data-privacy-bill-david-stauss-5nqdc.

[90] For detailed analysis of the amendments to the CTDPA, see Bailey Sanchez, Felicity Slater & Chloe Altieri, *Connecticut Shows You Can Have It All*, FPF (June 9, 2023), https://fpf.org/blog/connecticut-shows-you-can-have-it-all. SB 3 also added new protections for "consumer health data," which is discussed in more detail in the next subsection.

Focusing on the youth privacy amendments, SB 3 added novel business obligations for controllers offering any online product, service, or feature to individuals whom the controller has actual knowledge or wilfully disregards are minors under the age of 18. Such controllers must:

- Use reasonable care to avoid "any heightened risk of harm to minors" caused by their product, service, or feature;[91] and
- Conduct a data protection assessment that meets the requirements of the CTDPA and additionally addresses (A) the purpose of the product, service, or feature, (B) the categories of minors' personal data processed, (C) the purposes for processing such data, and (D) any reasonably foreseeable heightened risk of harm to minors resulting from offering the product, service, or feature.

Further, unless consent is obtained, controllers must ***not***—

- Process personal data
    - for targeted advertising, sale of personal data, or profiling in furtherance of fully automated consequential decisions;
    - unless reasonably necessary to provide a product, service, or feature,
    - for any processing purpose other than what was disclosed at the time of collection or what is reasonably necessary for or compatible with the disclosed processing purpose; or
    - for longer than necessary to provide the online product, service, or feature;
- Use a "system design feature to significantly increase, sustain or extend any minor's use of such online service, product, or feature"; or
- Collect a minor's precise geolocation data unless such data is reasonably necessary to provide the online product, service, or feature and the controller provides a signal indicating to the minor that it is collecting precise geolocation data.

In 2024, the Colorado General Assembly passed SB 41, which amended the Colorado Privacy Act to add youth privacy protections similar to those in Connecticut SB 3.[92] The Virginia General Assembly similarly passed HB 707, which added youth privacy protections to the VCDPA which are more modest than those in Connecticut SB 3 or Colorado SB 41 and are focused on expanding risk assessment requirements and minimizing the use of children's data.[93]

---

[91] Heightened risk of harm to minors is defined to mean "processing minors' personal data in a manner that presents any reasonably foreseeable risk of (A) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors, (B) any financial, physical or reputational injury to minors, or (C) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person" This term is defined consistently with the specific examples of "heightened risk of harm to a consumer" which are the triggers for conducting data protection assessments under the CTDPA. In contrast to more expansive youth privacy laws, such as California's Age-Appropriate Design Code, the harms to minors under SB 3 are tied to traditional privacy harms that do not involve content or proxies for content, which could allay some of the Constitutional concerns that have plagued other youth privacy laws.

[92] Bailey Sanchez & Daniel Hales, *Little Users, Big Protections: Colorado and Virginia Pass Laws Focused on Kids Privacy*, FPF (May 20, 2024), https://fpf.org/blog/little-users-big-protections-colorado-and-virginia-pass-laws-focused-on-kids-privacy.

[93] *Id.*

2. Consumer Health Data Protections

States have taken an increasingly fractured approach to protecting health data in recent years. As seen in Table 5 (Appendix), state lawmakers have devised a variety of articulations for health data subject to sensitive data protections, shifting from an early focus on "mental or physical health diagnosis" to more recently also include conditions, treatment, and various other formulations. One notable addition in recent years is the term "consumer health data," which comes with a number of new business obligations.

Connecticut SB 3, in addition to its increased protections for adolescent data, expanded the definition of sensitive data under the CTDPA to include "consumer health data," defined as personal data used by a controller to identify a consumer's physical or mental health diagnosis or condition, including gender-affirming health data and reproductive or sexual health data. SB 3 likewise added new business obligations with respect to consumer health data. These protections apply to "persons"—a broader category than "controllers" which includes non-profits and small businesses who are otherwise exempt from the CTDPA.[94] The law provides that these covered entities ***cannot***:

- Provide employees or contractors with access to consumer health data unless that recipient is subject to a statutory or contractual duty of confidentiality;
- Provide processors with consumer health data unless the contractor is bound by the contract required under the CTDPA;
- Geofence mental, reproductive, or sexual health facilities (within a boundary of 1,750 feet) for identifying, tracking, or collecting data or sending notifications to an individual about their consumer health data; or
- Selling or offering to sell consumer health data without obtaining opt-in consent.

Maryland's comprehensive privacy law, enacted in 2024, included Connecticut-style consumer health data protections.

3. Biometrics

Like with health data, biometric data has long been an established category of sensitive data under state privacy laws. Nevertheless, state lawmakers are exploring heightened protections for biometrics that go above-and-beyond opt-in consent requirements. In 2024, Colorado enacted HB 1130, which amended the Colorado Privacy Act to add rights and obligations influenced by those under the Illinois Biometric Information Protection Act (BIPA).[95] HB 1130 extends obligations beyond the covered entity thresholds in the Colorado Privacy Act, applying to any entity collecting biometric data, including employers. HB 1130 also adds heightened business

[94] SB 3's application to "persons" is representative of a broader trend whereby state laws are imposing specific obligations on entities that would otherwise be exempt from the law. For example, SB 3 imposes consumer health data obligations on "persons" who do not otherwise meet the controller requirements. Texas, Nebraska, and Minnesota restrict small businesses—who are otherwise exempt from their laws—from selling sensitive data without an individual's consent. In 2024, Colorado amended the Colorado Privacy Act to add protections for employee biometrics.
[95] H.B. 1130, 2024 Reg. Sess., (Colo. 2024).

obligations (e.g., biometric policies, retention requirements, security breach protocols, collection restrictions, sharing limitations, and nondiscrimination provisions) and new individual access rights with respect to biometric data. As of November 2024, the Colorado Attorney General has already commenced rulemaking related to the amendment's implementation.[96]

E. New Individual Rights

States are also innovating with expanding the individual data rights to new contexts. Most notably, this includes a right to know the identity of third-parties receiving your personal data and a right to contest adverse profiling decisions.

1. Right to Know Specific Third-party Recipients of Personal Data

In 2023, Oregon became the first state to expand the individual's right of access to require controllers to disclose the list of "specific third parties" to whom the controller disclosed either (i) the individuals' personal data, or, at the controller's discretion, (ii) any personal data.[97] Delaware enacted a similar right that allows individuals to "[o]btain a list of the *categories* of third parties to which the controller has disclosed the consumer's personal data."[98] Delaware's right is narrower than Oregon's in that it provides the right to obtain a list of the *categories* of third party recipients rather than the *specific* recipients; however, the right is also stronger than Oregon's in that the controller must provide a list personalized to the individual making the request, whereas under Oregon's law the controller can opt to provide a longer, non-personalized list of all third-party recipients.

In 2024, Maryland enacted a narrower version of Delaware's right, allowing individuals to access the "categories" of third parties to which the controller disclosed the individual's personal data or the categories of third parties to whom the controller disclosed any consumer's personal data if the controller does not maintain that information in a format specific to one individual.[99] In 2024, Minnesota became the second state to provide the Oregon-style right to know specific third-party recipients.[100]

These expanded rights of access in Oregon, Delaware, Maryland, and Minnesota are distinct from the common business obligation in many of the state comprehensive privacy laws to include the categories of third party recipients of personal data in a privacy notice. Rhode Island has taken a slightly different approach to try and achieve a similar result. Rather than providing this expanded individual right to access, the RIDTPPA includes a novel business obligation requiring that, in their privacy notice, a controller must list "all third parties to whom the controller has sold or may sell customers' personally identifiable information." This requirement could be more difficult to operationalize than the access right in Oregon and Minnesota, and it raises questions about

[96] Colo. Off. Att'y Gen., *2024 Colorado Privacy Act Rulemaking*, https://coag.gov/colorado-privacy-act-rulemaking (last visited Nov. 6, 2024).
[97] Or. Rev. Stat. § 646A.574 (1)(a)(B) (2023).
[98] Del. Code tit. 6, § 12D-1047(a)(5) (emphasis added).
[99] S.B. 541, 2024 Reg. Sess., § 14–4605(B)(6) (Md. 2024).
[100] 2024 Minn. Laws Ch. 121, https://www.revisor.mn.gov/laws/2024/0/Session+Law/Chapter/121.

whether a company is prohibited from selling personally identifiable information to new recipients who were not identified in the notice at the time of collection.

2. Right to Contest Adverse Profiling Decisions

Use of automated decisionmaking technology to make or facilitate consequential decisions poses a variety of privacy, civil rights, and due process risks.[101] State comprehensive privacy laws typically already provide a right for individuals to opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects.[102] The Minnesota Consumer Data Privacy Act (MNCDPA), which was enacted in May 2024, became the first state comprehensive privacy law to include a novel right to contest adverse profiling decisions. Under the provisions, if a consumer's personal data is profiled in furtherance of legal or similarly significant decisions, then the consumer has the right to:

- Question the result of the profiling.
- Be informed of
  - the reason that the profiling resulted in the decision, and
  - if feasible, be informed of
    - what actions the consumer might have taken to secure a different decision and
    - the actions that the consumer might take to secure a different decision in the future.
- Review the consumer's personal data used in the profiling.
- If the decision is determined to have been based upon inaccurate personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated.[103]

Some lawmakers have responded further to these increased risks stemming from automated decisionmaking technology, in part by introducing bills that regulate the development and deployment of such tools. In 2024, Colorado enacted an anti-discrimination law regulating the development and deployment of high-risk artificial intelligence systems used to make certain consequential decisions concerning individuals.[104]

Narrow Definitions of "Personal Data" Might Weaken Profiling Safeguards: Although the rights to opt-out of and contest certain profiling decisions include decisions that result in the provision or denial by the controller of employment opportunities, employee data is not within the scope of personal data under the law. This makes it unclear to what degree the opt-out and contestment rights apply in employment contexts.

---

[101] Future of Privacy Forum, *Unfairness by Algorithm: Distilling the Harms of Automated Decision-making*, FPF (Dec. 2017), https://fpf.org/wp-content/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf.
[102] *E.g.*, Colo. Rev. Stat. § 6-1-1306(1)(a)(I) (2023); Conn. Gen. Stat. § 42-518(a)(5) (2023); S.B. 541, 2024. Reg. Sess., § 14–4605(B)(7)(III) (Md. 2024).
[103] 2024 Minn. Laws Ch. 121, https://www.revisor.mn.gov/laws/2024/0/Session+Law/Chapter/121.
[104] Tatiana Rice, Keir Lamont & Jordan Francis, *The Colorado Artificial Intelligence Act*, FPF (July 2024), https://fpf.org/wp-content/uploads/2024/07/FPF-Legislation-Policy-Brief_-The-Colorado-AI-Act-Final.pdf.

Conclusion

While attempts at passing federal privacy legislation have stalled, state lawmakers have stepped in and responded to the privacy risks present in the processing of Americans' personal data. In the span of six years, the state privacy law landscape has exploded in depth and complexity as nineteen states have enacted comprehensive consumer privacy laws.

By distilling this broad landscape to construct the "anatomy" of state comprehensive privacy law, this report highlights the strong commonalities and the nuanced differences between the various laws, showing how they can exist within a common, partially-interoperable framework while also creating challenging compliance difficulties for companies within their overlapping ambits. Unless and until a federal privacy law materializes, this ever changing state landscape will continue to evolve as lawmakers iterate upon the existing frameworks and add novel obligations, rights, and exceptions to respond to changing societal, technological, and economic trends.

If you have any questions, please contact us at info@fpf.org.

Disclaimer: This report is for informational purposes only and should not be used as legal advice.

Appendix

Table 1. List of State Comprehensive Privacy Laws as of September 2024

State	Title	Enacted	FPF Analysis
California	California Consumer Privacy Act (CCPA) • Regulations (2023) • California Privacy Rights Act (CPRA) (2020)	2018	Blog Post
Virginia	Virginia Consumer Data Protection Act (VCDPA) • 2022 Amendments - HB 308 - HB 714 / SB 534 • 2024 Amendment (HB707)	2021	Blog Post 2024 Amendment
Colorado	Colorado Privacy Act (CPA) • Regulations (2023) • 2024 Amendments (Youth; Biometrics; Biological Data)	2021	Blog Post Children's Data Amendment
Utah	Utah Consumer Privacy Act (UCPA)	2021	Blog Post
Connecticut	Connecticut Data Privacy Act (CTDPA) • 2023 Amendment (Children; Health)	2022	Blog Post 2023 Amendment
Iowa	N/A (SF 262)	2023	Blog Post
Indiana	Indiana Consumer Data Protection Act (ICDPA)	2023	Blog Post
Montana	Montana Consumer Data Privacy Act (MCDPA)	2023	Blog Post
Tennessee	Tennessee Information Protection Act (TIPA)	2023	Blog Post
Florida[105]	Florida Digital Bill of Rights (FDBR)	2023	Blog Post
Texas	Texas Data Privacy and Security Act (TDPSA)	2023	Blog Post
Oregon	Oregon Consumer Privacy Act (OCPA)	2023	Blog Post
Delaware	Delaware Personal Data Privacy Act (DPDPA)	2023	Blog Post
New Jersey	N/A (S332)	2024	Blog Post
New Hampshire	N/A (SB 205) • 2024 Amendment (HB 1220)	2024	Blog Post
Kentucky	Kentucky Consumer Data Protection Act (KCDPA)	2024	LinkedIn

[105] Not counted as one of the nineteen state comprehensive privacy laws for this report.

State	Title	Enacted	FPF Analysis
Nebraska	Nebraska Data Privacy Act (NDPA)	2024	LinkedIn
Maryland	Maryland Online Data Privacy Act (MODPA)	2024	Blog Post
Minnesota	Minnesota Consumer Data Privacy Act (MNCDPA)	2024	Blog Post
Rhode Island	Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)	2024	Blog Post

Table 2. At a Glance: CCPA v. WPA Framework

See Part I.A

Table 3. Categorization of Cure Periods

See Part I.B.5

Table 4. Controller Applicability Thresholds

State	Population (2023)[106]	Thresholds	High %	Low %	Enacted
California[107]	38.97 million	100,000	0.26%	N/A	2018
Virginia	8.72 million	100,000 / 25,000	1.15%	0.29%	2021
Colorado	5.88 million	100,000 / 25,000	1.70%	0.43%	2021
Utah[108]	3.42 million	100,000 / 25,000	2.93%	0.73%	2021
Connecticut	3.62 million	100,000 / 25,000	2.76%	0.69%	2022
Iowa	3.21 million	100,000 / 25,000	3.12%	0.78%	2023
Indiana	6.86 million	100,000 /25,000	1.46%	0.36%	2023
Montana	1.13 million	50,000 / 25,000	4.41%	2.21%	2023
Tennessee[109]	7.13 million	175,000 / 25,000	2.46%	0.35%	2023
Texas*	30.50 million	N/A	N/A	N/A	2023

[106] All population values were taken using the 2023 values from the following table: U.S. Dept. Ag., *Population*, https://data.ers.usda.gov/reports.aspx?ID=17827 (last visited July 29. 2024).
[107] The CCPA has three alternative thresholds for coverage. Cal. Civ. Code § 1798.140, subd. (d)(1).
[108] Businesses must also have annual revenue of at least $25,000,000 to be covered.
[109] Businesses must also have annual revenue of at least $25,000,000 to be covered.

State	Population (2023)[106]	Thresholds	High %	Low %	Enacted
Oregon	4.23 million	100,000 / 25,000	2.36%	0.59%	2023
Delaware	1.03 million	35,000 / 10,000	3.39%	0.97%	2023
New Jersey	9.29 million	100,000 / 25,000	1.08%	0.27%	2024
New Hampshire	1.40 million	35,000 / 10,000	2.50%	0.71%	2024
Kentucky	4.53 million	100,000 / 25,000	2.21%	0.55%	2024
Nebraska*	1.98 million	N/A	N/A	N/A	2024
Maryland	6.18 million	35,000 / 10,000	0.57%	0.16%	2024
Minnesota*[110]	5.74 million	100,000 / 25,000	1.74%	0.44%	2024
Rhode Island	1.10 million	35,000 / 10,000	3.19%	0.91%	2024

Table 5. Sensitive Data Elements

Sensitive Data Elements: Personal data that reveals, includes, or is—	States
Social security, driver's license, state identification card, or passport number	CA
Log-in, financial account, debit card, or credit card in combination with any required security or access code, password, or credentials allowing access to an account	CA
Financial information (which shall include a consumer' account number, account log-in, financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account)	NJ
Precise [specific] geolocation data: radius ≤ 1,750 feet	VA, UT, CT, IA, IN, MT, TN, TX, OR, DE, NJ, NH, KY, MD, RI
Precise geolocation: radius ≤ 1,850 feet	CA
Specific geolocation data: information that directly identifies geographic coordinates with an accuracy of more than three decimal degrees of latitude and longitude (or equivalent in alternative geographic coordinate system) or a street address derived from the coordinates.	MN
Racial or ethnic origin	CA, VA, CO, UT, CT, IA, IN, MT, TN, TX, OR, DE, NJ, NH, KY, NE, MD, MN, RI
National origin	OR, MD

[110] The MNCDPA includes numerical thresholds and a Texas-style small business exception.

Sensitive Data Elements: Personal data that reveals, includes, or is—	States
Citizenship or immigration status	CA, VA, UT, CT, IA, IN, MT, TN, TX, OR, DE, NJ, NH, KY, NE, MD, MN, RI
Citizenship or citizenship status	CO
Religious beliefs	CA, VA, CO, UT, CT, IA, IN, MT, TN, TX, OR, DE, NJ, NH, KY, NE, MD, MN, RI
Philosophical beliefs	CA
Union membership	CA
Contents of a consumer's mail, email, and text messages (unless the business is the intended recipient of the communication)	CA
Genetic data	CA, OR, DE, MD
Genetic data (processed for the purpose of uniquely identifying a natural person)	VA, UT, CT, IA, IN, MT, TN, TX, NH, KY, NE, MN, RI
Genetic data (that may be processed for the purpose of uniquely identifying an individual)	CO, NJ
Biometric data	OR, DE
Biometric information (processed for the purpose of uniquely identifying a consumer)	CA, VA, UT, CT, IA, IN, MT, TN, TX, NH, KY, NE, MN, RI
Biometric data (that may be processed for the purpose of uniquely identifying an individual)	CO, NJ, MD
Biological data ("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, singly or in combination with other personal data, for identification purposes") which includes neural data ("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")	CO
Neural data (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)	CA
Personal information collected and analyzed concerning a consumer's health	CA
Mental or physical health diagnosis	VA, IA, TN, TX, KY, NE
Mental or physical health diagnosis made by a healthcare provider	IN
Mental or physical health condition or diagnosis	CO, CT, MT, OR, NH, MN
Mental or physical health condition or diagnosis (including pregnancy)	DE
Mental or physical health condition, treatment, or diagnosis	NJ

Sensitive Data Elements: Personal data that reveals, includes, or is—	States
Information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a healthcare professional	UT
Consumer health data (defined term)	CT, MD
Personal information collected and analyzed concerning a consumer's sex life or sexual orientation	CA
Sexual orientation	VA, UT, IA, IN, TN, OR, KY, NE, MN
Sex life or sexual orientation	CO, CT, MT, DE, NJ, NH, MD, RI
Sexuality	TX
Personal data [collected] from [of] a known child	VA, CO, CT, IA, IN, MT, TN, TX, DE, NJ, NH, KY, NE, MN, RI
Is a child's personal data	OR
Personal data of a consumer that the controller knows or has reason to know is a child	MD
Status as transgender or non-binary	OR, DE, NJ, MD
Status as a victim of crime	OR, CT

Table 6. Data Minimization Standards

See Part II.C

Table 7. Teenager Opt-in Requirements

See Part II.D.1

1350 Eye Street NW Suite 350
Washington, DC 20005

info@fpf.org

FPF.org