Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

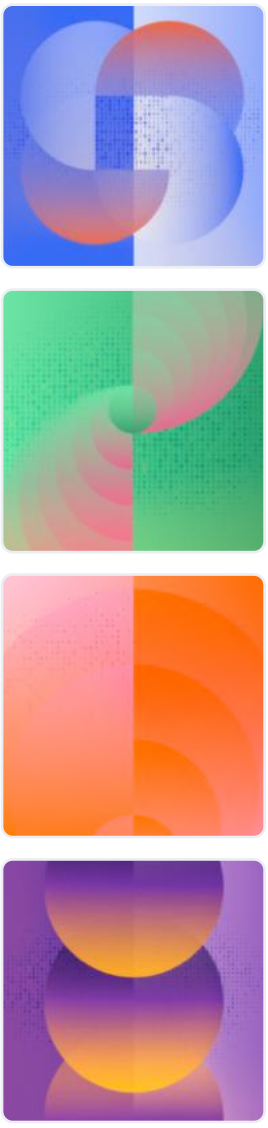
ccianet.org

2024

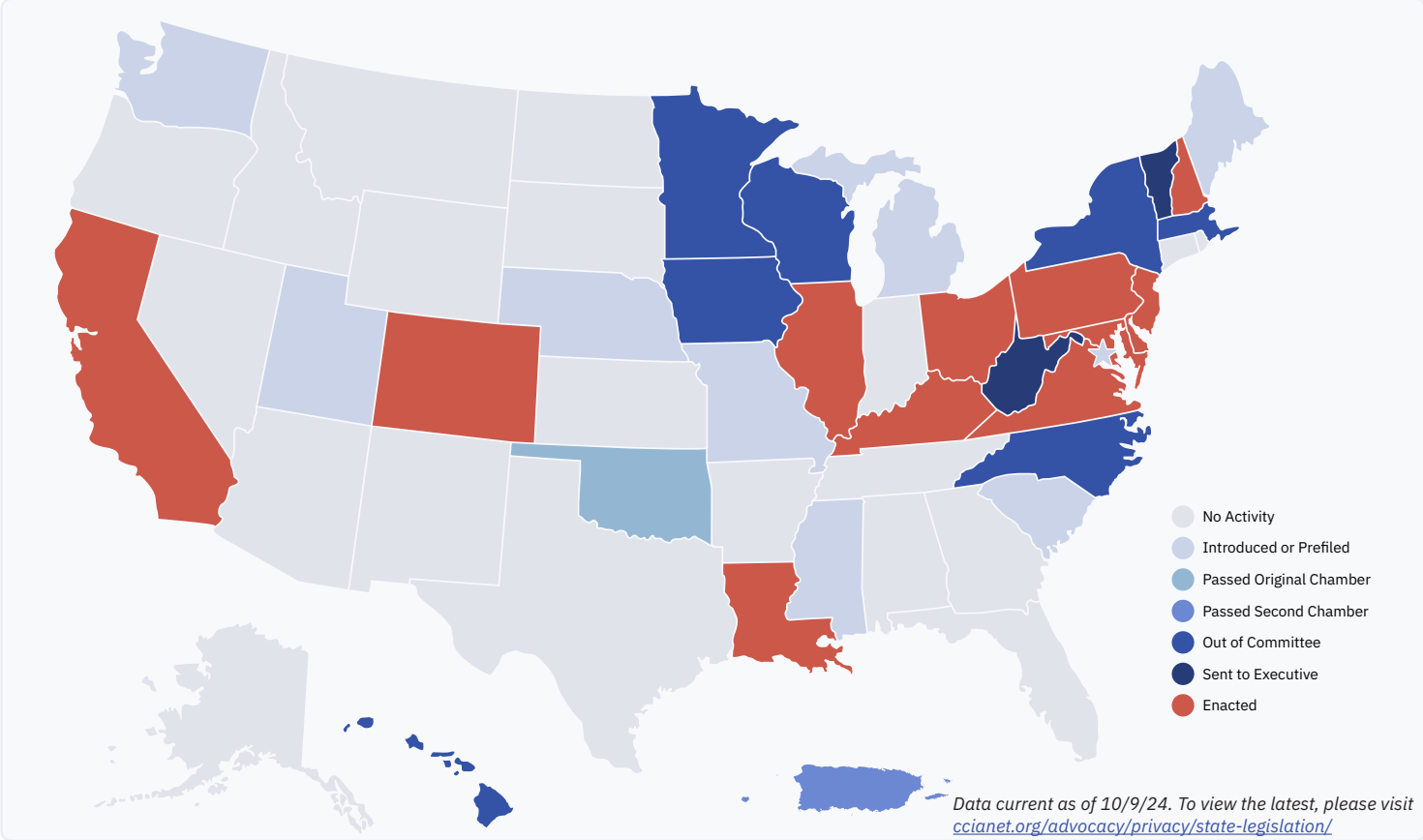
State Landscape Privacy

State Landscapes 2024

Each year, CCIA's State Policy Center releases a series of policy overviews outlining the major trends across the 50 state legislatures, while also highlighting key states expected to be active in the upcoming session. In recent years, many state legislatures have considered various proposed laws that would significantly impact the technology industry. As legislators often borrow or mimic ideas and legislation from other states throughout the country, observing the trends found in this year's legislative efforts will help prepare for future policy engagements. Monitoring trends in individual state capitals across the country can be instructive of policy developments more broadly. Particularly for policies that could threaten innovation and the tech ecosystem, it is important to consider and be prepared to engage in such consequential policy conversations.



2024 State Privacy Landscape



Data current as of 10/9/24. To view the latest, please visit ccianet.org/advocacy/privacy/state-legislation/

In recent years, Congress has considered several iterations of a comprehensive federal privacy law to provide consistent protections for consumers across the United States. However, efforts to pass such legislation have faced significant challenges and remain ongoing. In the absence of a national standard, a growing number of state lawmakers have introduced legislative measures to establish baseline consumer data protections. California was the first state to enact such legislation in 2018; since then, 19 other states have enacted their own laws, including Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia. Just this past legislative session, Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Rhode Island joined the pack.

While there are variations among state privacy laws, a general consensus has emerged in favor of promoting interoperability and alignment with other jurisdictions. Many states have chosen to harmonize key definitions and business obligations, fostering a more consistent regulatory landscape. Maryland, however, has taken a divergent path with its strict data minimization requirements. This approach could inadvertently stifle innovation and business activity within the state by limiting the flexibility of covered entities to leverage collected data for new and potentially beneficial purposes.

Maine and Vermont also grappled with the complexities of drafting privacy legislation that deviated significantly from existing laws. These states ultimately faced challenges in achieving

legislative consensus, with Maine failing to pass a bill and Vermont's proposal being vetoed by Governor Phil Scott (R). As New England consumers often cross state lines, harmonization of privacy laws is essential to ensure that businesses can readily comply across jurisdictions and consumers understand their privacy rights.

Other states have taken a more sectoral approach in addressing aspects of privacy, such as protections specific to health and biometric data in Washington, or for younger users in Connecticut and Virginia.

Given the steady momentum across state legislatures, in Democrat- and Republican-led states alike, states will almost certainly continue to advance consumer privacy laws. It remains to be seen whether these new laws will align with existing frameworks or diverge and create an increasingly complex patchwork, complicating roadmaps for businesses to comply.

Types of Data Privacy Measures

1 Comprehensive Consumer Data Privacy

U.S. privacy law today consists of various disparate federal and state laws. However, this data privacy framework significantly changed in 2019, when the California Consumer Privacy Act (CCPA) went into effect, which created a significant compliance burden for most businesses. Since then, state-level activity has increased as more states look to establish data privacy laws in the absence of a comprehensive federal law. Twenty states have now enacted comprehensive consumer data privacy laws. Many of these laws adopt similar definitions, business obligations, and consumer rights, allowing for covered entities to leverage compliance regimes across multiple states.

Examples:

- KY HB 15
- ME LD 1977
- MD SB 541/HB 567
- MN HF 4757
- NE LB 1074
- NH S. 255
- NJ S. 332
- RI S.2500/H.7787
- VT H. 121

Impact:

CCIA has concerns over the adoption of jurisdiction-specific legislation because a divergent set of state privacy laws can result in a confusing and burdensome regulatory patchwork. A uniform federal approach to consumer privacy is necessary to ensure that businesses know how to meet their compliance obligations and consumers are able to understand and exercise their rights. By enacting comprehensive federal privacy legislation with state-to-state consistency, we promote a trustworthy information ecosystem. Thus, rules should be normative rather than prescriptive– they should set standards of conduct that must be followed rather than endorse or condemn any specific feature or design choice. Confining the rules to today's practices necessarily invites circumvention through invention and will quickly render the rules obsolete.

Biometric Information / Health Data / Neural Data

Prevents private entities from collecting biometric information without disclosure and consent. Biometrics are measurements related to a person's unique physical characteristics, like fingerprints or retinal measurements. A person's biometric data can be used as unique identifiers and allow for automatic recognition. Thus, as biometric data becomes more prevalent, laws are being introduced to restrict private entities. Such proposals often include restrictions on the use of precise geolocation data. More recently, states have taken these restrictions a step further, focusing on "health data" and "neural data" as well.

Where:

- CA SB 1223
- CO HB 24-1058
- DC B25-0930

Impact:

Prohibiting the use of biometric info except when "strictly necessary" could deny consumers innovative products in the marketplace. Thus, it is important to balance protecting consumers with providing a clear roadmap for innovative businesses to comply with. Legislation should strive to be technology-neutral to avoid creating barriers to innovation and prevent skewing the competitive playing field.

Data Protections for Younger Users

Prohibits an operator of an internet website, online service, or mobile application from certain activities when minors are involved. Such legislation creates privacy rights which restrict the advertising of specific products and services to minors. At the Federal level, the Children's Online Privacy Protection Act was passed in response to the growth of internet marketing techniques that targeted children and collected their personal information from websites without any parental notification. These measures may also require businesses that provide online services, products, or features likely to be accessed by children to comply with vague standards or outright ban children from accessing certain platforms.

Where:

- VA HB 707/SB 361
- NY S.7695B/A.8149A

Impact:

Responsible digital services support, and are engaged in advancing, the important goal of proactively protecting children online. Such bills should minimize subjectivity, provide enough compliance guidance to avoid requiring organizations to collect more information about children, and avoid restricting the use of tools and settings, that help protect all users, including children. At a minimum, proposed laws should include cure provisions that allow companies to correct and come into compliance.

Key States

California

While California was the first state to establish a comprehensive state privacy law, the rulemaking process led by the California Privacy Protection Agency is ongoing with a new formal rulemaking comment period likely forthcoming in Fall 2024 on insurance, cybersecurity audits, risk assessments, and automated decision-making technologies. California state lawmakers continue to introduce and advance legislation to amend various aspects of the state's current privacy law, including measures focused on protections specific to children, opt-out mechanisms, and artificial intelligence training data. With no sign of slowing down, monitoring these ongoing developments, including any new legislation during the 2025 legislative session, will be critical.

Massachusetts

The Massachusetts Legislature once again considered several bills concerning consumer data privacy protections, though none of them advanced during the formal session, which concluded at the end of July. Unlike most state legislatures, Massachusetts operates under a full-year legislative session. While the likelihood of these bills advancing in the remainder of the year is slim, there is still the possibility of some movement. If these measures do not advance during 2024, they likely will be reintroduced when the new biennium begins in January 2025.

Maine

The Maine Legislature advanced a data privacy proposal, LD 1977, which diverges from other existing state privacy laws. The proposal advanced in the House, but failed to garner support in the Senate, where many members were concerned about the bill's strict data minimization provisions and the associated impact on businesses in addition to the types of exemptions the proposal provided. Although the 2024 bill's sponsor is term-limited, the Legislature will very likely reignite conversations in 2025 given the amount of focus it gave the bill this year.

New York

The New York Senate once again passed a comprehensive data privacy bill in the final weeks of their legislative session, though the bill did not make it through the Assembly before the session ended. The primary driver of data privacy in the Legislature, Sen. Kevin Thomas (D), opted to not run for re-election this year, so the bill will have a new Senate sponsor next year, potentially Sen. Kristen Gonzalez (D), the Senate Internet and Technology Committee chair.

Key States

Vermont

The Vermont Legislature passed a data privacy proposal, H. 121 that, like the proposal in Maine, diverged from the model used by over a dozen other states. Although the bill received broad support in both chambers, Gov. Phil Scott (R) vetoed the bill, citing concerns about the impact of a private right of action on businesses, as well as lack of interoperability with other states given Vermont's smaller size. The House voted to override the Governor's veto, but the Senate failed to do so, and ultimately the bill died. Given all of the movement during the 2024 session, Vermont will almost certainly take up a data privacy proposal again in 2025.

Recent Reports

A Comprehensive Look at New Developments in Data Privacy Laws

Coblentz Patch Duffy & Bass LLP

Coblentz Patch Duffy & Bass LLP published *A Comprehensive Look at New Developments in Data Privacy Laws* which includes an overview of newly enacted privacy laws, effective dates and applicability thresholds, an update on California's draft risk assessment and automated decision making regulations, in addition to trends regarding protections specific to children's online protections and health data, and enforcement.

This report is available at: https://www.jdsupra.com/legalnews/2024-mid-year-privacy-report-a-6572458/

How Americans View Data Privacy

Pew Research Center

Pew Research Center published a report, *How Americans View Data Privacy*, providing insights to how surveyed Americans view the role of social media, tech companies, and government regulation as well as Americans' day-to-day experience with online privacy. The survey also focuses on artificial intelligence and survey participants' perspectives on its role in data collection.

This report is available at: https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/#role-of-social-media-tech-companies-and-government-regulation

2024 State Landscape
Challenges Presented by Proposed Bills

The Normative vs Prescriptive Approach

Privacy frameworks should provide appropriate protections for consumers while maintaining competition and fostering innovation. Thus, any privacy legislation should set forth principles rather than prescriptions. There is a risk of obsolescence when rules embrace prescriptive over normative guidance. For example, when legislation gets too prescriptive, it risks locking in existing technology and practices, resulting in the short shelf-life of rules. To put it simply, a prescriptive framework may be inapplicable to later technological developments. Overly prescriptive rules might inadvertently give advantage to established firms by erecting barriers to entry as well.

Technology-Neutral Legislation

Privacy legislation should remain technology-neutral and flexible, which allows regulations to continue to operate effectively as technology evolves. Technology-neutral laws also promote growth and innovation by avoiding rigid provisions. The neutral language gives clarity to investors and users of new technology regarding how it will be regulated, which encourages innovation. For example, with a technology-neutral approach, regulators do not need to change regulations too often to keep up with technological development, which is called "future-proofing regulation." Because technology tends to outpace the legislative process, a regulatory approach without technology-neutral language could lead to picking "winners and losers" among technologies and business models. Thus, laws that mention specific technologies are bound to become obsolete, whereas tech-neutral laws can apply to future innovations.

Opt-out Mechanisms and Consent Fatigue

Consent mechanisms can be a powerful tool for promoting transparency and consumer control. However, requiring specific user-consent for all data collection or processing would be inconsistent with consumer expectations and likely overwhelm them, resulting in "consent fatigue." Thus, regulations should limit the number of consent requests and allow customers to opt in/reverse any opt out selection. Absent these requirements, multiple entities may create competing signals with different standards. As a result, businesses and customers would suffer from significant confusion about how to exercise their opt-out rights.

Federal Preemption / Patchwork

CCIA supports comprehensive federal privacy legislation that includes clear and consistent consumer privacy rights and responsibilities for organizations that collect/process data. A uniform federal approach for consumer privacy protection is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to understand and exercise their rights. While CCIA supports state efforts to implement comprehensive privacy laws, it is important to remember that until a federal privacy law is enacted, America's industries must comply with a growing number of state laws that often adopt disparate standards for addressing the same issues. State-to-state consistency is a valuable goal for both industry and consumers.

Enforcement

CCIA supports investing exclusive enforcement authority with the state attorney general. However, many state proposals include new private rights of action. States adopting such enforcement regimes risk opening their state courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive, and these costs may be passed on to consumers, disproportionately impacting smaller businesses and startups across the state. Furthermore, every state that has established a comprehensive consumer data privacy law has invested enforcement authority with its state attorney general. This allows for the leveraging of technical expertise concerning enforcement authority, foregrounding the public interest.

Testimony and Written Comments

This table provides details about written comments and testimony submitted by CCIA in 2024.

State	Bill	Date	Product/Stance
California	AB 1008	9/6/2024	AB 1008 seeks to alter the definition of "publicly available information" in such a way that would create uncertainty and confusion as to which types of data formats the CCPA covers. CCIA joined coalition efforts to oppose this legislation. Gov. Newsom signed the bill into law.
California	AB 1949	3/5/2024 9/6/2024	AB 1949 would amend existing state law to generally prohibit the collection, sharing, sale, use, or disclosure of data for consumers under 18 years of age, absent affirmative consent. CCIA joined coalition efforts to oppose this legislation. Gov. Newsom vetoed the bill.
California	AB 3048	3/26/2024	AB 3048 would effectively require universal opt-out mechanisms under the California Consumer Privacy Act (CCPA) to transmit consumers' opt-out preferences to businesses that they interact with online. The bill undermines user choice and goes beyond the CCPA by mandating such a signal. AB 3048 was vetoed by Gov. Newsom.
California	AB 3124	4/8/2024	AB 3124 proposes unrealistic requirements regarding publicly displaying personal information on internet websites. CCIA opposed the bill, highlighting that the broad definition of "covered personal information" would prevent users from sharing information such as known relatives, or date of birth. This is information that users may want to hide, and have tools to do so, but also may want to share with others, including social connections. AB 3124 failed to advance during the 2024 legislative session.

State	Bill	Date	Product/Stance
California	SB 1223	4/8/2024	SB 1223 would define "sensitive personal information," for purposes of the CCPA, to additionally include a consumer's neural data, and would define "neural data" to mean information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from non neural information. CCIA joined coalition efforts to oppose this legislation. Gov. Newsom signed the bill into law.
California	CPPA Board	1/25/2024	Amidst the California Privacy Protection Agency's (CPPA) ongoing rulemaking process, CCIA submitted a reaction letter to the CPPA Board reiterating several outstanding concerns regarding rulemaking discussions about automated decision-making technologies, risk assessments, and cybersecurity audits.
Colorado	HB 24-1058	1/29/2024	Gov. Jared Polis (D) signed HB 1058 into law on April 17, 2024. The bill expands the definition of "sensitive data" to include biological data. The legislation also specifies that "biological data" includes neural data, which is information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device. CCIA adopted an "oppose, unless amended" position.
Maryland	SB 541	2/9/2024 3/26/2024	On May 9, 2024 Gov. Wes Moore signed SB 541, the Maryland Online Data Privacy Act, into law. Maryland's law includes strict and restrictive provisions concerning data minimization and may prevent covered businesses from using collected data in new and potentially-beneficial ways. CCIA opposed SB 541 with written and virtual testimony throughout the session.
Maryland	HB 567	2/9/2024 3/21/2024	On May 9, 2024 Gov. Wes Moore signed HB 567 into law. This is the companion bill to SB 541. CCIA opposed HB 567 with written and virtual testimony throughout the session.
Rhode Island	HB 7787 S. 2500	3/27/2024 3/19/2024	On June 26, 2024 HB 7787 became law without the Governor's signature. CCIA provided written comments in support of the bill.
Vermont	H. 121	5/30/2024 2/7/2024	This legislation proposes comprehensive consumer data privacy protections. CCIA was opposed to this bill as it was not interoperable with other existing state privacy laws and included a private right of action.
Virginia	SB 252	1/31/2024	SB 252 would amend the Virginia Consumer Data Protection Act to impose additional requirements and prohibitions on controllers regarding "cookies." CCIA opposed this bill. SB 252 was continued to 2025 in General Laws and Technology.