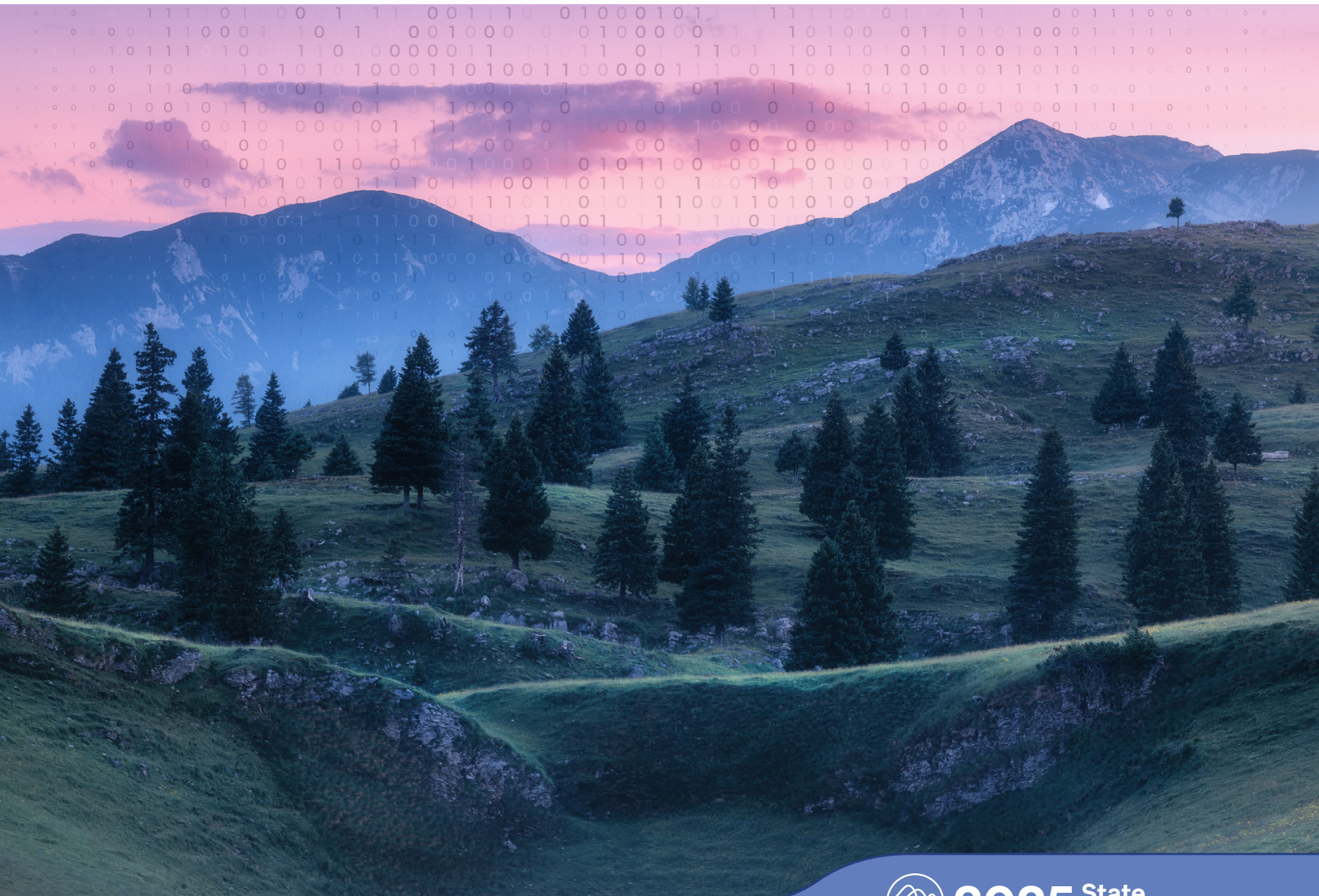
Computer & Communications Industry Association

Open Markets. Open Systems. Open Networks.

ccianet.org

2025

State Landscape
Privacy



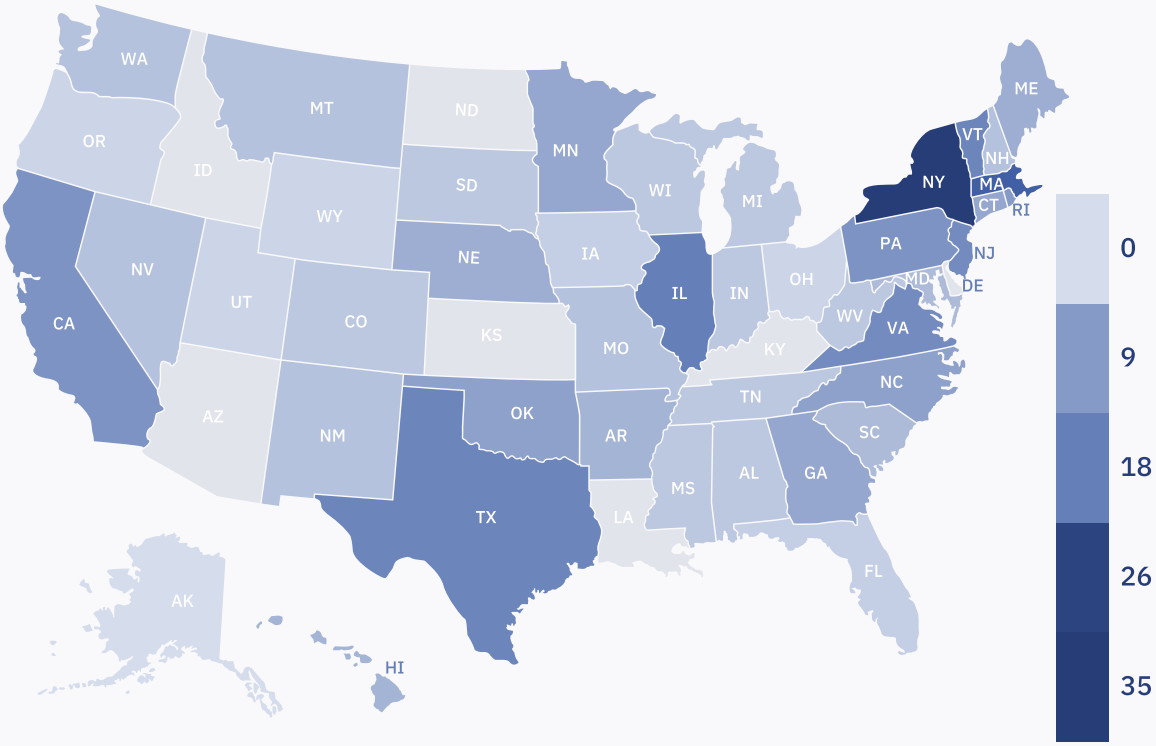
2025 State Landscapes

Privacy

State Landscapes 2025

Each year, the Computer & Communications Industry Association (CCIA) State Policy Center releases policy overviews outlining 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.

State Privacy Landscape 2025



Includes carryover legislation from 2024 and new legislation in 2025.
Data current through 9/30/2025.

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, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia. Surprisingly, no new comprehensive privacy laws have passed in 2025 as of October 1, 2025. However, states have continued proposing new privacy legislation and measures in Massachusetts, New York, and Pennsylvania have the potential to pass in 2025 or the 2026 session.

Three significant trends have emerged during the 2025 legislative session. First, states have pushed for "meaningful transparency," requiring privacy policies contain easy to find, understandable, and clear terms. This includes mandates for short-form privacy notices that summarize key data practices. Second, states have sought to increase protections for minors beyond existing state privacy laws and the

federal Children's Online Privacy Protection Act (COPPA). Proposed measures often include provisions to limit or ban targeted advertising to minors, as well as new requirements that online services be designed with children's best interests in mind. Finally, several states have amended their existing comprehensive privacy laws. These amendments frequently addressed technical ambiguities, closed potential loopholes, and clarified the scope of business obligations, signaling a maturation of the state legislative landscape.

While there are variations among state privacy laws, a general consensus has emerged in favor of promoting alignment across jurisdictions. This has led to the harmonization of key definitions and business obligations, such as the right to access, correct, and delete data, and the establishment of a universal opt-out mechanism for targeted advertising. Maryland, however, has taken a divergent path with its strict data minimization requirements, which limit the collection and use of consumer data to only what is strictly necessary to provide a specific product or service. This approach could inadvertently stifle innovation and business activity within the state by limiting covered entities' ability to use consumer data to improve their products and services, in stark contrast to the more permissive frameworks of other states.

While a federal privacy law remains elusive, states continue to push new privacy legislation and refine existing laws. The trends of increased transparency, enhanced protections for minors, and the continuous amendment of prior legislation show a dynamic and evolving state privacy landscape.

Types of State 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) took effect, creating significant compliance burdens 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.

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 contradictory regulatory framework. 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

Biometric data laws generally restrict private entities' ability to collect 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 its collection. More recently, states have taken these restrictions a step further, focusing on "health data" and "neural data" as well.

Impact:

Prohibiting the use of biometric info except when "strictly necessary" could deny consumers innovative products and services. Regulations should therefore provide a clear roadmap for innovative businesses to comply with while maintaining consumer protections. 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

Some privacy laws prohibit an operator of an internet website, online service, or mobile application from certain activities when minors are involved. Often, these laws restrict the advertising of specific products and services to minors. At the federal level, COPPA 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. However, 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 online services.

Impact:

Responsible digital services implement measures to proactively protect children online. Youth privacy protections should minimize subjectivity, avoid forcing 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 time to correct and come into compliance.

Key States

California

While California established the first comprehensive state privacy law, the rulemaking process led by the California Privacy Protection Agency is ongoing, with the California Consumer Privacy Act's formal rulemaking period continuing through 2025. California state lawmakers continue to introduce and advance legislation to amend the state's current privacy law, including measures focused on children's privacy, opt-out mechanisms, and artificial intelligence training data. With no sign of slowing down, monitoring these ongoing developments, including any new legislation during the 2025-2026 legislative session, will be critical. Governor Newsom recently signed AB 566 (California Opt Me Out Act), AB 656 (Account Cancellation), and SB 361 (Defending Californians' Data Act) into law.

Massachusetts

The Massachusetts Legislature once again considered several bills concerning consumer data privacy protections, though none advanced to the floor during the first half of the legislative session. Unlike most state legislatures, Massachusetts operates under a full-year legislative session. While the likelihood of these bills advancing in 2025 is slim, some movement remains possible. If these measures do not advance during 2025, they likely carry over to the 2026 session.

Vermont

Vermont was the first state to enact a law regulating data brokers in 2018, but does not currently have a comprehensive privacy law. The Vermont Data Privacy Act, passed by both the House and the Senate in 2024, was ultimately vetoed by the Governor. During the 2025-2026 legislative session S.71 and H.208, both titled "An act relating to consumer data privacy and online surveillance" were introduced but ultimately failed to pass. Passing a comprehensive Privacy law is considered a main priority of Representative Monique Priestley in the 2026 session.

Recent Reports

Anatomy of State Comprehensive Privacy Law: Surveying the State Privacy Law Landscape and Recent Legislative Trends

November 2024 | Future of Privacy Forum

The full report is available here.

The report includes an overview of comprehensive privacy laws enacted from 2018-2024. It summarizes the landscape and identifies the "anatomy" of state privacy law.

2025 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. When legislation gets too prescriptive, it risks locking in existing technology and practices, and the law's utility will be short-lived. 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, allowing regulations to continue operating 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, a concept known as "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, or to 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

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 clear and consistent compliance obligations and that consumers can understand and exercise their rights. While CCIA supports state efforts to implement comprehensive privacy laws, legislators should recognize that until a federal privacy law is enacted, America's industries must increasingly comply with disparate standards across the country. 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. Investing enforcement authority with the state attorney general allows states to leverage technical expertise concerning privacy harms and foreground the public interest.

Table 1. Testimony and Written Comments Submitted by CCIA in 2025 (Effective 9/30/25)

State	Bill/Topic	Date(s)	Product/Stance
Arkansas	HB 1717	3/18/25	HB 1717 created the Arkansas Children and Teens' Online Privacy Protection Act and was signed into law by Governor Sarah Huckabee Sanders. CCIA opposed this measure.
California	CPPA Proposed Rules	1/14/25 5/30/25	On July 24, 2025, the California Privacy Protection Agency (Agency) Board adopted regulations that (1) updated existing CCPA regulations; (2) implemented requirements for certain businesses to conduct risk assessments and complete annual cybersecurity audits; (3) implemented consumers' rights to access and opt—out of businesses' use of ADMT; and (4) clarified when insurance companies must comply with the CCPA.
California	AB 322	7/8/25	Failed to pass, carries over to 2026 session.
California	AB 566	3/11/25	Signed into law, effective January 1, 2027.
California	AB 1355	3/26/25 4/15/25	Failed to pass, carries over to 2026 session.
Colorado	Privacy Act Rules	7/10/25	The Colorado Attorney General's Office has released final revisions to their proposed rules amendments for SB24-041 (2024), a set of child privacy amendments to the Colorado Privacy Act.
Illinois	SB 50	3/28/25	Failed to pass, carriess over to 2026 session.
Maryland	HB 1365	2/28/25	Failed to pass.
Massachusetts	S 2619	9/30/25	In second chamber awaiting consideration.
Nebraska	LB 504	1/31/25	Signed into law, effective January 1, 2026.
New Jersey	Privacy Act Rules	8/27/25	The New Jersey Attorney General's Office has released its draft regulations implementing the New Jersey Data Privacy Act.
Rhode Island	H 5830	4/1/25	Failed to pass.
South Carolina	S 268	4/2/25	Failed to pass, carries over to 2026 session.
Utah	HB 418	3/12/25	Signed into law, section 13-75-301 effective May 7, 2025. All other sections effective July 1, 2026.
Vermont	HB 210	2/28/25	Failed to pass, carries over to 2026 session.
Vermont	SB 69	2/21/25 4/7/25 5/30/25	Signed into law, Sec. 1, 9 V.S.A. § 2449f(b) and 9 V.S.A. § 2449g(b) (rulemaking authority) effective July 1, 2025. All other sections effective January 1, 2027.
Vermont	SB 71	3/7/25	Failed to pass, carries over to 2026 session.
Virginia	SB 1023	1/28/25	Failed to pass.

Table 2. 2025 and 2026 Regulatory Timetable (Effective 9/30/25)

2025 Date	State(s)	Type of Regulatory Event
January 1	Colorado	Mandatory notice of violation and right to cure period expires.
January 1	Connecticut, Texas	Opt-out preference signals for targeted advertising/sale go into effect.
January 1	Connecticut	Mandatory right to cure period expires (AG discretion to grant cure period).
January 1	Delaware, Iowa, Nebraska, New Hampshire	Goes into effect.
January 1	Montana, Minnesota	Data protection assessment requirements apply to processing activities created/generated after this date.
January 1	Montana, New Hampshire	Opt-out preference signals for targeted advertising/sale go into effect.
January 1	Texas	Authorized agent provisions go into effect.
January 15	New Jersey	Goes into effect.
July 1	Colorado	Obligations regarding the collection and processing of biometric data go into effect.
July 1	Delaware	Data protection assessment requirements apply to processing activities created/generated after this date.
July 1	Oregon	Goes into effect date for 501(c)3 tax exempt organizations.
July 1	Tennessee	Goes into effect.
July 31	Minnesota	Goes into effect.
October 1	Colorado	Obligations for data controllers that provide online services/products/features to minors go into effect.
October 1	Maryland	Goes into effect.
October 1	Maryland	Data protection assessment requirements apply to processing activities created/generated after this date.
October 1	Maryland	Opt-out preference signals for targeted advertising/sale go into effect.
December 31	Delaware, New Hampshire	Mandatory right to cure period expires (AG discretion to grant cure period).
December 31	Indiana	Data protection assessment requirements apply to processing activities created/generated after this date.
2026 Date	**State(s)**	**Type of Regulatory Event**
January 1	Delaware	Requirement to honor universal opt-out signals goes into effect.
January 1	Indiana, Kentucky, Rhode Island	Goes into effect.
January 1	Minnesota, Oregon	Mandatory right to cure period expires.
January 1	Oregon	Opt-out preference signals for targeted advertising/sale go into effect.
January 1	Rhode Island	Data protection assessment requirements apply to processing activities created/generated after this date.
April 1	Montana	Mandatory right to cure period expires.
June 1	Kentucky	Data protection assessment requirements apply to processing activities created/generated after this date.