Computer & Communications Industry Association

Open Markets. Open Systems. Open Networks.

ccianet.org

2026

State Landscape
Privacy

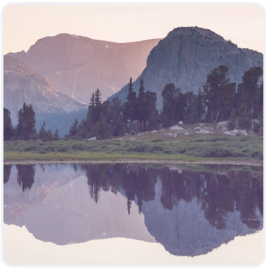


2026 State Landscapes

Privacy

Introduction

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. State legislatures considered a substantial volume of proposed privacy laws in 2026 that would significantly affect the technology industry, and the pace of enactment accelerated sharply compared to the prior year. 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.









2026 Overview

In recent years, Congress has considered several iterations of a comprehensive federal privacy law to provide consistent protections for consumers across the United States. Those efforts have continued to face significant challenges, and no federal framework advanced in 2026. In the absence of a national standard, state lawmakers kept filling the gap and did so at a pace not seen since 2023.

After a comparatively quiet 2025, in which no state enacted a new comprehensive consumer privacy law, four states enacted comprehensive privacy statutes in 2026: Oklahoma, Alabama, Louisiana, and Vermont. Oklahoma became the 20th state with a comprehensive privacy law when Governor Kevin Stitt signed SB 546 on March 20, capping a seven-year legislative effort. Alabama Governor Kay Ivey signed the 21st such law, the Alabama Personal Data Protection Act (HB 351), on April 17. Louisiana Governor Jeff Landry signed the 22nd, the Louisiana Data Privacy Act (SB 386) on May 29, and Vermont Governor Phil Scott signed the 23rd, the Data Privacy and Online Surveillance Act (S 71), on June 16. CCIA flagged Vermont's law as a top priority to watch in last year's Privacy Landscape.

These 23 states include Indiana, Kentucky, and Rhode Island, whose previously enacted laws took effect January 1, 2026. (This count follows IAPP's widely used tracking methodology, which excludes the Florida Digital Bill of Rights from the "comprehensive" category because it applies only to a narrow set of the largest technology companies. Trackers that include Florida will show 24.)

States also continued to amend their existing comprehensive laws. Connecticut's governor signed SB 4 on May 27, adding data broker registration requirements to the Connecticut Data Privacy Act despite a CCIA veto request. Maryland's HB 711 became law without the governor's signature on May 31, expanding the state's

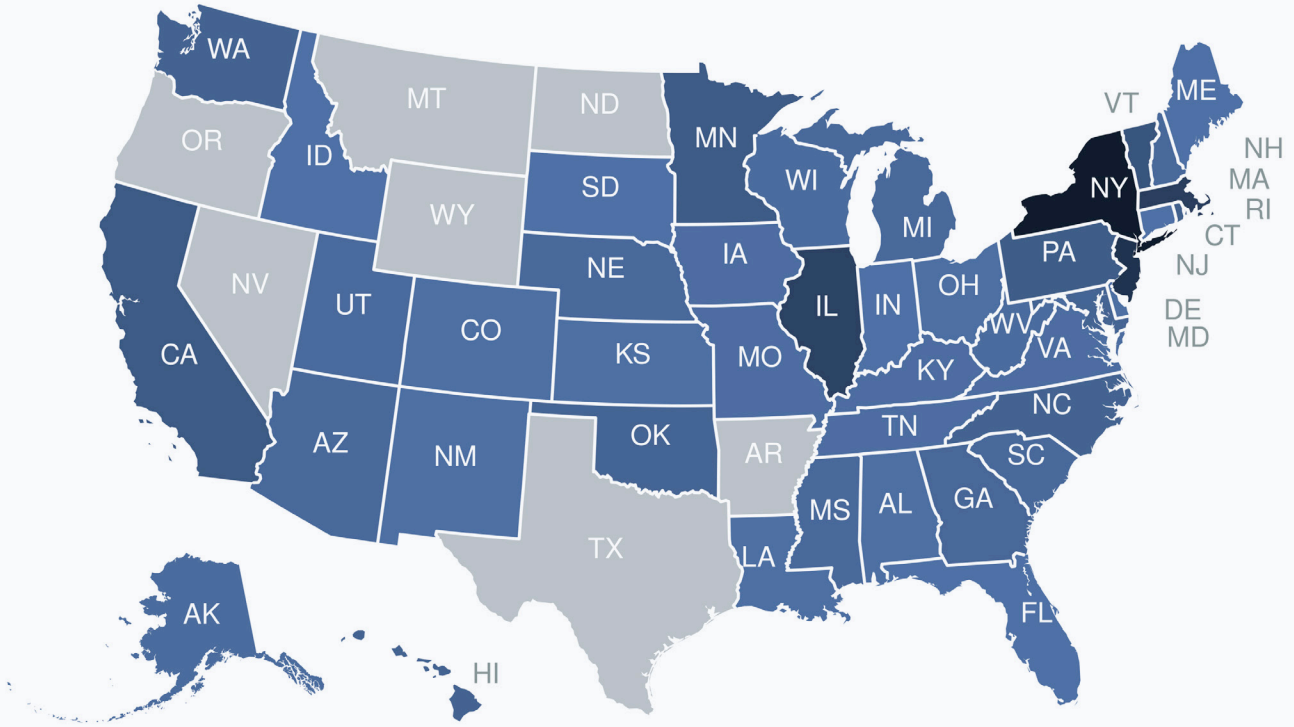
2026 Overview

definition of sensitive data to include inferences made from such data, and restricting data sales to government entities supporting civil immigration enforcement. New Hampshire governor Kelly Ayotte signed HB 1460 on June 19, adding new restrictions on the sale of personal data. Meanwhile, the Delaware legislature passed the year's most sweeping amendment, HB 380, which lowered the Delaware Personal Data Privacy Act's applicability thresholds, narrowed its financial-institution exemption, and imposed new third-party contracting and due-diligence duties. Governor Matt Meyer signed the bill on September 2, following veto requests CCIA and other industry coalitions submitted in July.

Massachusetts, a state CCIA flagged as a likely mover in last year's Landscape, came closer than ever to enacting a comprehensive law. The Senate unanimously passed its bill (S 2619) in September 2025, the House unanimously passed a companion version (H 5479) on June 4, 2026, and a six-member conference committee will work through the fall to reconcile the two bills before sending a compromise to Governor Healey. Pennsylvania's HB 78 likewise advanced further than in prior sessions, clearing the House and reaching the Senate floor for a second consideration before the year's activity wound down.

For businesses operating nationwide, this evolving regulatory landscape presents growing compliance challenges. Although most state laws continue to share a common foundation, individual states increasingly differ in definitions, thresholds, exemptions, consent requirements, data minimization standards, and obligations governing emerging technologies. This year's laws illustrate the risk concretely: Alabama omits data protection impact assessments entirely, Louisiana uses a revenue-based applicability test that departs from the consumer-count thresholds used in many other states, and Vermont imposes geofencing and consumer health data rules with no size threshold at all.

The Comprehensive Privacy Map Continues to Expand



Includes carryover legislation from 2025 and new legislation in 2026.
Data current through 9/30/2026.

The most visible development in 2026 was the continued geographic expansion of comprehensive privacy legislation, demonstrating that state-level privacy legislation remains a bipartisan and durable policy issue.

Four states enacted comprehensive privacy laws during the year:

- Alabama enacted the Alabama Personal Data Protection Act, effective May 1, 2027.
- Louisiana enacted the Louisiana Data Privacy Act, effective January 1, 2027.
- Oklahoma enacted its comprehensive privacy law, effective January 1, 2027.
- Vermont enacted the Vermont Data Privacy and Online Surveillance Act, effective January 1, 2028.

Together, these laws bring the number of states with enacted comprehensive privacy statutes to 23 (24, under trackers that also count Florida). While the laws differ in important respects, each builds upon the basic framework that has emerged across state privacy legislation.

New Laws Continue to Follow a Common Framework — With Important Differences

The newest comprehensive privacy laws continue to rely on the controller/processor framework that has become standard across the states. Consumers are generally given rights to access their information, request deletion or correction, and opt out of certain uses of their data. Businesses are generally subject to obligations concerning data security, transparency, sensitive data, and consumer requests.

Louisiana's new law, for example, applies to businesses meeting specified revenue or data-processing thresholds and provides consumer rights concerning access, correction, deletion, and opting out of personal data sales. The law is enforced by the Attorney General and provides covered businesses a 30-day right to cure window before enforcement actions can be brought.

Alabama similarly adopted a comprehensive framework but includes its own applicability thresholds, exemptions, and enforcement provisions. The Alabama Attorney General is responsible for enforcement, and the law provides a 45-day cure window.

Vermont's law represents a somewhat different approach. The Vermont Data Privacy and Online Surveillance Act combines comprehensive privacy protections with provisions concerning online surveillance and data use. Vermont also grants more stringent protections for some types of data, classifying all consumer health and neural data as sensitive data.

Existing Privacy Laws Are Becoming More Complex

While four states adopted comprehensive privacy laws in 2026, the more consequential trend for businesses may be the growing number of states modifying laws that are already on the books.

States are increasingly revisiting their existing privacy statutes to address perceived gaps, respond to enforcement experience, and regulate specific technologies and data practices. These developments demonstrate a fundamental shift in state privacy policy: increasingly, the policy debate concerns not whether a state should have a privacy law, but how that law should operate, what data and technologies it should cover, and how far it should depart from the emerging national framework.

Key States



Connecticut

Connecticut significantly amended its privacy framework through SB 4, which became Public Act 26-64. The legislation added several new requirements to the Connecticut Data Privacy Act. Among other provisions, the law established a data broker registration system and centralized deletion mechanism, expanded protections involving profiling, restricted the sale, sharing, transfer, or access to precise geolocation data, and established new requirements concerning facial recognition technology.

CCIA engaged extensively on SB 4. CCIA supported the goal of strengthening consumer privacy protections while recommending targeted amendments to avoid conflicting requirements and unnecessary competitive disadvantages. CCIA specifically raised concerns regarding the breadth of the data broker definition and provisions concerning personalized algorithmic pricing.



Delaware

Delaware also substantially modified its existing comprehensive privacy framework when HB 380 was signed into law on September 2. The law now extends to smaller businesses, narrows certain exemptions, imposes additional contractual requirements for disclosures of personal data to third parties, and strengthens protections relating to profiling.

CCIA raised concerns that HB 380 would move Delaware away from the emerging consensus among state privacy laws without meaningfully improving consumer privacy. CCIA specifically highlighted provisions concerning the definition of a sale of personal data and third-party disclosures, and warned that the additional requirements could place Delaware at a competitive disadvantage.

Privacy Regulation Moves Beyond Comprehensive Privacy Laws

The 2026 legislative session also demonstrated that comprehensive privacy statutes are only one part of the state privacy landscape.

States increasingly considered legislation addressing individual categories of data and particular technologies. These measures often operate independently of a state's comprehensive privacy law and can impose separate requirements.

Precise Geolocation

Precise geolocation emerged as an increasingly prominent privacy issue in 2026.

Connecticut's SB 4 prohibits controllers and third parties from selling precise geolocation data. Massachusetts's pending Consumer Data Privacy Act would go further still: both the Senate-passed S 2619 and the House-passed H 5479 include a blanket ban on the sale of precise geolocation data, a provision the conference committee is expected to retain in whatever compromise reaches Governor Healey's desk.

The growing focus on location data reflects a broader policy trend: lawmakers are moving beyond general definitions of personal information and increasingly identifying particular types of information as deserving heightened protections.

Data Brokers and Deletion

Data brokers were another major focus in 2026.

Connecticut established a state data broker registry and an accessible deletion mechanism through SB 4.

California continued implementation of its Delete Act and its centralized Delete Request and Opt-Out Platform, or DROP. The California Privacy Protection Agency is responsible for implementing the Delete Act. The Delete Act's registration and accessible deletion mechanism requirements became effective January 1, 2026. California SB 923 updated language around consumer privacy requests regarding data deletion records. SB 923 was signed into law and goes into effect January 1, 2027.

New Jersey enacted the year's most expansive data broker legislation. Signed June 30 as A 5328, the law establishes a public registry administered by the Division of Consumer Affairs and imposes annual registration fees ranging from $5,000 to $1.5 million depending on the volume of consumer data a business sells (by far the steepest fee structure of any state data broker law). The Act also introduces a category with no precedent in any other state's data broker statute: the "data collector," a business that collects data directly from its own customers and later sells or licenses it to a data broker, which is now subject to the same registration regime as data brokers themselves. Separately, the law amends the New Jersey Data Privacy Act to prohibit all entities doing business in New Jersey from selling sensitive data, regardless of whether they qualify as controllers. This provision carries civil penalties of $50,000 per record sold. Registration itself remains inoperative until March 27, 2027, with the Division targeting a spring 2027 launch of the registry.

These developments suggest that data brokers will remain an important target of state privacy legislation, particularly as policymakers consider how consumers can exercise deletion rights across multiple companies with which they may have no direct relationship.

Co-Regulation of Privacy and AI

One of the most important developments in 2026 was the growing overlap between privacy legislation and artificial intelligence policy.

AI systems rely on data to train, operate, personalize, and improve their functionality. As a result, lawmakers increasingly turned to privacy concepts, including data minimization, consent, profiling, transparency, and sensitive data, when considering how AI should be regulated.

This convergence was visible in Connecticut, where lawmakers considered consumer privacy legislation alongside broader AI and online safety proposals. CCIA's testimony emphasized that privacy regulation should provide meaningful consumer protections without creating overlapping or contradictory obligations for businesses.

California's regulatory framework provides another example. Regulations governing automated decision-making technology under the California Consumer Privacy Act (CCPA) became effective January 1, 2026, with compliance and audit deadlines phasing in through 2030. The regulations address consumer rights to access and opt out of certain uses of automated decision-making technology, along with risk assessments and cybersecurity audits.

The convergence of privacy and AI raises important policy questions for states. A law intended to regulate AI may impose privacy obligations even when its primary objective is algorithmic accountability, while a privacy law may increasingly govern how businesses use AI to make decisions.

Children and Privacy Remain a Major Focus

Children's privacy remained among the most active areas of state technology legislation in 2026.

Rather than relying solely on expanding data protections for children, lawmakers increasingly considered:

- age assurance and age verification;
- parental consent;
- restrictions on targeted advertising;
- data minimization for minors;
- children's interactions with AI and chatbots;
- digital age assurance codes;
- social media restrictions; and
- restrictions on the collection or use of children's sensitive information.

These proposals frequently overlap with comprehensive privacy legislation and online safety measures, creating another layer of regulatory complexity. A company may face one set of requirements under a state's comprehensive privacy law, another under a children's privacy statute, and additional requirements under an online safety or AI law.

CCIA's 2026 advocacy reflected this convergence, including engagement on proposals involving age verification, children's privacy, parental consent, online services, and AI-powered technologies.

Universal Opt-Outs and Consumer Choice

Universal opt-out mechanisms also continued to gain prominence in 2026.

States increasingly require covered businesses to recognize mechanisms that allow consumers to communicate their privacy preferences without making individual requests to every company. California, Colorado, Connecticut, Delaware, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Minnesota, Maryland, and Texas are among the states with requirements addressing universal opt-out mechanisms.

The continued expansion of universal opt-out requirements illustrates the broader movement toward making privacy rights easier for consumers to exercise. However, differences in how states define, implement, and enforce those requirements create additional operational challenges for businesses.



California: From Privacy Legislation to Privacy Regulation

California remained the nation's most active state privacy jurisdiction in 2026.

The California Privacy Protection Agency continued implementing and enforcing CCPA and the Delete Act while overseeing a growing body of privacy regulations. Major CCPA regulations concerning risk assessments, cybersecurity audits, and automated decision-making technology became effective January 1, 2026.

The Agency also continued exploring additional areas for future rulemaking. During 2026, preliminary rulemaking activities addressed:

- Delete Request and Opt-Out Platform audits;
- employee data;
- notices and disclosures;
- reducing friction in exercising privacy rights; and
- opt-out preference signals.

The CPPA's work demonstrates how state privacy regulation is entering a more mature phase. Rather than simply establishing statutory rights, California is developing detailed administrative requirements governing how those rights are implemented in practice.

CCIA's engagement in California reflected this broad range of issues. 31 of CCIA's 62 privacy engagements during 2026 involved California, making the state the largest focus of CCIA's privacy advocacy.

CCIA's California engagement included legislative testimony, written comments, coalition advocacy, and engagement on issues ranging from privacy and geolocation to children's privacy, age assurance, AI, automated technologies, and emerging data practices.

CCIA's 2026 Privacy Advocacy

CCIA remained actively engaged with state policymakers throughout 2026, providing written comments, testimony, coalition letters, plus-one letters, and veto requests. This advocacy focused on preserving meaningful consumer privacy protections while encouraging policymakers to adopt practical, technology-neutral requirements that can be implemented consistently across jurisdictions.

CCIA PRIVACY ENGAGEMENT IN 2026

62 TOTAL ENGAGEMENTS

14	24	16	10	12
States	Public Comments	Coalition Letters	Plus-One / Me-Too	Testimony / Veto Requests

CCIA's state advocacy addressed both traditional privacy legislation and the growing number of technology policy proposals that incorporate privacy requirements.

Engagement Breakdown: 24 public comments, 16 coalition letters, 10 plus-one / me-too letters, 8 testimony appearances, and 4 veto requests across 14 states, reconciled against the underlying 2026 engagement log.

A Growing Patchwork of Privacy Requirements

The cumulative effect of these developments is an increasingly fragmented state regulatory environment.

The broad architecture of state privacy law remains relatively consistent. Most comprehensive laws provide consumers with some combination of access, correction, deletion, and opt-out rights. Most also impose obligations concerning transparency, data minimization, security, sensitive data, and consumer requests.

But important differences remain. States vary in:

- applicability thresholds;
- definitions of personal and sensitive data;
- consent requirements;
- treatment of publicly available information;
- exemptions;
- universal opt-out requirements;
- data protection assessments;
- profiling and automated decision-making;
- children's data;
- employee data;
- enforcement mechanisms; and
- rulemaking authority.

As more states amend existing laws, these differences are becoming increasingly significant.

The result is a regulatory environment in which businesses cannot simply determine whether a state has a privacy law. They must increasingly determine which specific data practices are covered, whether additional technology-specific laws apply, and whether state regulators have adopted implementing regulations.

Looking Ahead to 2027

The state privacy landscape is likely to remain highly active heading into 2027. Several developments will warrant particular attention.

1

Implementation of the newest comprehensive laws

Oklahoma, Louisiana, and Alabama will begin implementing their newly enacted privacy frameworks, while Vermont's law will take effect in 2028.

2

Continued amendments to existing privacy laws

States with laws already in effect are likely to continue revisiting them. The experience of Connecticut and Delaware demonstrates that the first generation of state privacy statutes is not necessarily the final version.

3

More privacy and AI convergence

As AI systems become more deeply integrated into consumer products and services, lawmakers will increasingly consider privacy, data governance, automated decision-making, and AI policy together.

4

Children's privacy and age assurance

Children's privacy is likely to remain one of the most active areas of state technology policy, particularly as lawmakers consider age assurance, parental consent, AI chatbots, social media, and targeted advertising.

5 Data brokers and deletion

Other states may follow the examples of California's DROP system and Connecticut's centralized deletion mechanism. New Jersey's registry, though not operative until March 2027, will be an early test of whether its unprecedented data-collector category and steep fee structure hold up to implementation and likely legal challenges.

6 Increasing regulatory enforcement

States with laws already in effect are likely to continue revisiting them. The experience of Connecticut and Delaware demonstrates that the first generation of state privacy statutes is not necessarily the final version.

Conclusion

The 2026 state privacy landscape demonstrates that the era of simply counting how many states have comprehensive privacy laws is giving way to a more complicated phase of privacy policymaking.

23 states now have comprehensive privacy laws on the books, but the similarities among those laws should not obscure their growing differences. States are increasingly using privacy laws to address specific categories of data, emerging technologies, children and teens, automated decision-making, data brokers, geolocation, and online services.

The practical effect for businesses operating nationally is a steadily rising compliance burden. A consistent national framework can provide consumers with meaningful privacy protections while reducing unnecessary regulatory fragmentation. Absent such a framework, CCIA will continue working with state policymakers to encourage privacy policies that are effective, technology-neutral, workable, and capable of supporting both consumer protection and continued innovation.

Table 1. Selected CCIA State Privacy Engagements in 2026 (Data current as of 9/15/26)

Reflects CCIA public comments, written and oral testimony, coalition letters, and veto requests on state privacy legislation and rulemaking.

State	Bill	Topic	Date(s)	Product/Stance
California	AB 2169	Digital Choice Act (interoperability)	4/13, 5/6/26	CCIA led coalition opposition to AB 2169's mandatory interoperability interface for social media platforms and AI model operators. Held under submission in Assembly Appropriations 5/14/26; failed upon adjournment.
California	AB 883	Data brokers: threatened elected officials and judges	1/12, 6/23/26	CCIA and coalition partners (TechNet) engaged in opposition testimony. Passed the Legislature 8/27. Signed into law by Governor Newsom 9/27/26.
California	AB 1159	CA Learner Personal Information Protection Act	1/9/26	CCIA opposed the bill's expansion of student privacy obligations to higher education and its new private right of action. Signed into law 9/10/26.
California	AB 1542	Sensitive personal information (sale/ share ban)	4/9, 5/20, 6/15, 8/17, 9/4/26	CCIA and coalition partners (CalChamber) opposed AB 1542's categorical ban on selling or sharing sensitive personal information; vetoed by Governor Newsom 9/27/26.
California	AB 2561	Privacy/data practices	4/2, 4/28/26	CCIA and TechNet initially opposed AB 2561 before removing opposition following amendments; Signed into law by Governor Newsom 9/27/26.
California	CPPA	Delete Request and Opt-Out Platform (DROP) audits rulemaking	5/7/26	CCIA submitted preliminary comments in response to the CPPA's invitation for comment on delete request and opt-out platform audits.
California	SB 923	Expanding Privacy Rights Act (deletion right)	3/27, 6/8, 6/17, 9/4/26	CCIA and coalition partners (CalChamber) opposed the CPPA-sponsored bill expanding the CCPA deletion right to third-party-sourced data. Signed into law by Governor Newsom 9/27/26.
California	SB 976	AADC / Protecting Our Kids from Social Media Addiction Act (rulemaking)	6/30/26	CCIA submitted written comments and oral testimony at the DOJ's June 30 public hearing on proposed AADC implementing regulations
California	SB 1130	Invasion of privacy: wearable recording devices	3/18, 6/17, 8/19, 9/8/26	CCIA and coalition partners (TechNet) raised concerns throughout the committee process. Passed the Legislature 8/31/26; Vetoed by Governor Newsom 9/30/26.
Connecticut	SB 4	CTDPA amendment (data broker registry)	3/3, 4/28, 5/5/26	CCIA opposed SB 4 and requested a veto. Signed into law by Governor Lamont 5/27/26.
Connecticut	SB 5	CART Act (AI, chatbots, online safety)	3/3/26	CCIA offered oral testimony jointly addressing SB 4 and SB 5. Signed into law by Governor Lamont as Public Act 26-15 on 6/2/26.
Delaware	HB 145	Reverse location / reverse keyword search warrants	7/14/26	CCIA requested a veto. Signed into law by Governor Meyer 9/9/26 despite CCIA's opposition.
Delaware	HB 380	DPDPA amendment (thresholds, exemptions, third-party duties)	4/29, 5/26, 6/9, 6/17/26	CCIA opposed HB 380 throughout the committee process and, with NetChoice and the U.S. Chamber, requested a veto. Signed into law by Governor Meyer 9/2/26 despite CCIA's veto request; effective 1/1/27.

State	Bill	Topic	Date(s)	Product/Stance
Illinois	SB 340	Comprehensive consumer privacy proposal	5/22/26; Privacy Panel testimony 4/10/26	CCIA opposed SB 340 and participated in the Illinois legislature's data privacy recommendations panel. Remains pending; Illinois has not enacted a comprehensive privacy law.
Maine	LD 1822	Maine Online Data Privacy Act	3/16/26	CCIA submitted comments opposing the bill. Failed upon adjournment.
Maryland	HB 1250	Curbing Harmful AI Technology Act (chatbots)	3/2/26	CCIA offered oral and written testimony opposing HB 1250 as inconsistent with the Maryland Online Data Privacy Act. Did not meet the crossover deadline; failed upon adjournment.
Maryland	SB 932	Social media platforms: display of user location	4/3/26	CCIA submitted comments (jointly addressing SB 932 and HB 883) warning that IP-based location display is inaccurate and could expose users to stalking or harassment. Passed the full Senate 42–0 on 3/23/26; failed upon adjournment.
Massachusetts	S 2619 / H 4746 / H 5479	Massachusetts Consumer Data Privacy Act	4/27, 7/7/26	CCIA and SIIA submitted joint comments and a joint letter. Senate passed S.2619 unanimously (9/25/25); House passed H.5479 unanimously (6/4/26); a conference committee is reconciling the two bills.
New Hampshire	HB 1589	Digital Choice Act (interoperability)	1/14/26	CCIA opposed HB 1589's mandatory interoperability interface for social media platforms. Failed upon adjournment.
New Mexico	SB 53	Comprehensive consumer privacy proposal	2/4/26	CCIA offered oral and written comments in opposition. Postponed indefinitely and failed upon adjournment.
New York	S 4609	Stop Online Predators Act (age verification)	3/31/26	CCIA submitted comments raising age-verification and default-settings concerns. The standalone bill remains in the Senate Finance Committee, but a version of its core provisions (the "Safe by Design" default-settings requirements) was separately enacted through the FY2027 state budget.
New York	S 9269 / A 10357	NY Health Information Privacy Act (NYHIPA)	5/20, 6/3, 8/4/26	CCIA and coalition partners opposed the revived NYHIPA and requested a veto. Passed both chambers 6/3–6/4/26; pending Governor Hochul's decision, following her December 2025 veto of the original bill.
Pennsylvania	HB 78	Comprehensive consumer privacy proposal	6/30/26	CCIA submitted comments. Passed the House and reached the Senate for second consideration (6/25/26); not yet enacted.
Vermont	S 71	Data Privacy and Online Surveillance Act (VDPOSA)	4/9/26	CCIA submitted comments during committee consideration, which raised major concerns with the private right of action provisions, and were ultimately removed from the original draft bill before being signed into law by Governor Scott 6/16/26; effective 1/1/28.
Virginia	SB 232	VCDPA amendment: minors, parental consent	2/4/26	CCIA submitted comments opposing expanded parental consent and data-access provisions. Continued to the 2027 session (15–0 vote).
Minnesota	SF 2940/ HF 2700	MCDPA amendment: consumer health data as sensitive data	3/11/26	CCIA submitted comments on the bill's expansion of sensitive data to include consumer health data. Both measures failed upon adjournment.

Table 2a. 2026 Regulatory Timetable (Data current as of 9/15/26)

Effective dates and regulatory milestones for comprehensive state privacy laws and major amendments.

2026 Date	State(s)	Type of Regulatory Event
January 1	Indiana, Kentucky, and Rhode Island	Comprehensive consumer privacy laws go into effect.
January 1	Delaware	Requirement to honor universal opt-out preference signals goes into effect.
January 1	Oregon	Opt-out preference signals for targeted advertising/sale go into effect; mandatory right-to-cure period expires.
January 1	Minnesota	Mandatory right-to-cure period expires.
January 1	Rhode Island	Data protection assessment requirements apply to processing activities created/generated after this date.
March 20	Oklahoma	Oklahoma Computer Data Privacy Act (SB 546) signed into law.
April 1	Montana	Mandatory right-to-cure period expires.
April 17	Alabama	Alabama Personal Data Protection Act (HB 351) signed into law.
May 27	Connecticut	SB 4 (data broker registration amendment to CTDPA) signed into law.
May 29	Louisiana	Louisiana Data Privacy Act signed into law.
May 31	Maryland	HB 711 (MODPA sensitive-data and immigration-enforcement amendment) becomes law without the Governor's signature; effective 7/1/26.
June 1	Kentucky	Data protection assessment requirements apply to processing activities created/generated after this date.
June 2	Connecticut	SB 5, the CART Act (AI, chatbots, online safety) signed into law as Public Act 26-15; provisions phase in through January 2028.
June 16	Vermont	Data Privacy and Online Surveillance Act (S.71) signed into law.
June 19	New Hampshire	HB 1460 (sale-of-data restriction amendment to NHDPA) signed into law.
July 1	Connecticut, Arkansas, and Utah	Amendments and comprehensive law provisions become effective / applicable.
July 1	Maryland	HB 711 amendments to the Maryland Online Data Privacy Act take effect.
August 1	California	Expanded Delete Act data broker registration and DROP-related requirements become operative.
September 2	Delaware	HB 380 (DPDPA amendment) signed into law by Governor Meyer, despite CCIA's veto request.
September 9	Delaware	HB 145 (reverse-location and reverse-keyword search warrant restrictions) signed into law by Governor Meyer, despite CCIA's opposition.

Table 2b. 2027-28 Regulatory Timetable (Data current as of 9/15/26)

Effective dates and regulatory milestones for comprehensive state privacy laws and major amendments.

2027 Date	State(s)	Type of Regulatory Event
January 1	Oklahoma	Oklahoma Computer Data Privacy Act becomes effective.
January 1	Louisiana	Louisiana Data Privacy Act becomes effective.
January 1	California	AB 566 (Opt Me Out Act — browser opt-out signals) and AB 1043 (Digital Age Assurance Act) become effective.
January 1	Delaware	HB 380 amendments to the DPDPA become effective.
January 1	Vermont	HB 211 data broker and edtech registration requirements (Sections 1 and 4) become effective.
May 1	Alabama	Alabama Personal Data Protection Act becomes effective.
July 31	Louisiana	Mandatory 30-day right-to-cure period sunsets.
2028 Date	**State(s)**	**Type of Regulatory Event**
January 1	Vermont	Data Privacy and Online Surveillance Act becomes effective.