LANDSCAPE

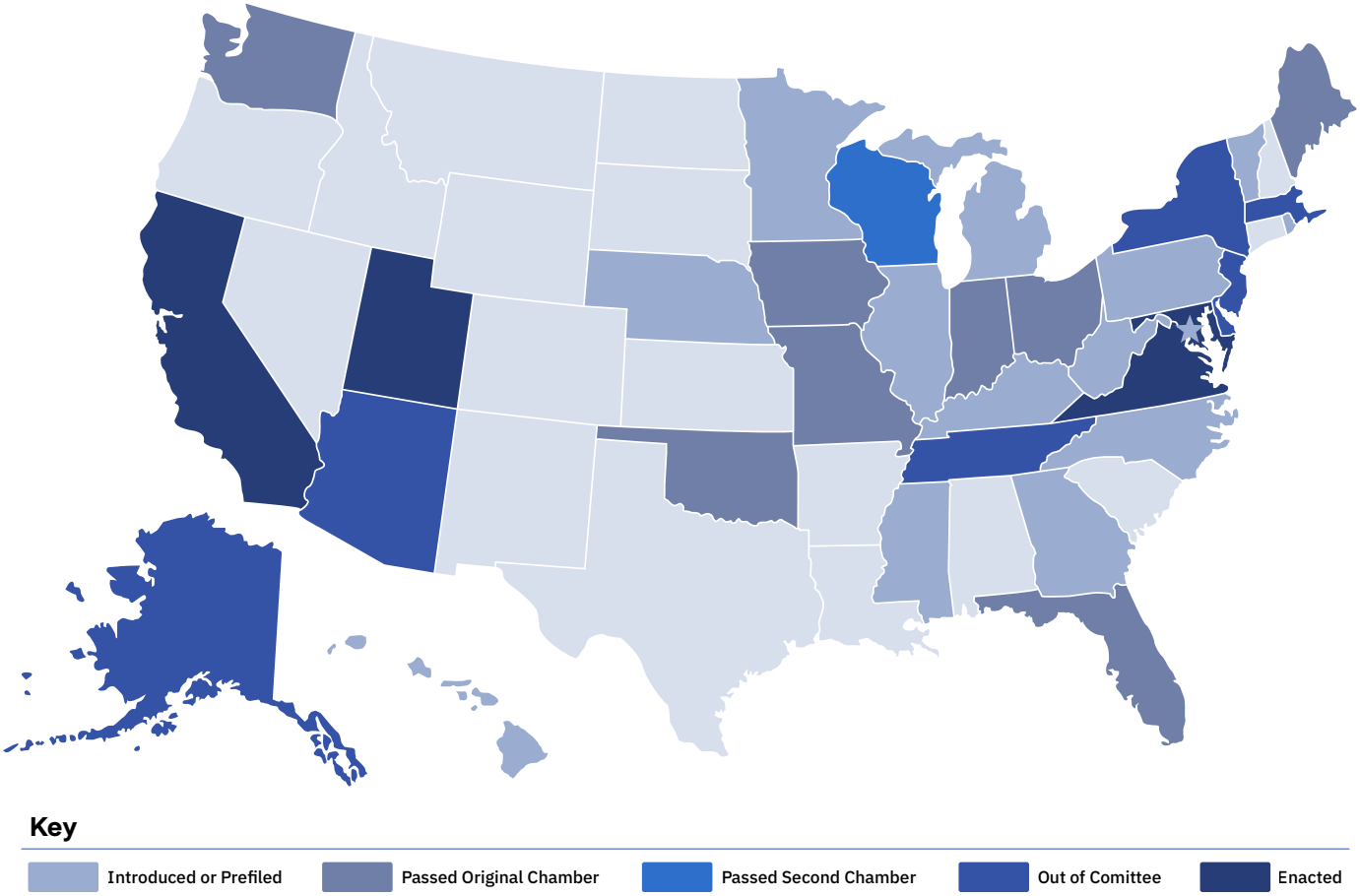
State Privacy Legislation

In the backdrop of the continuing impasse on federal privacy legislation, states began introducing measures aimed at addressing an array of data privacy concerns – ranging from bills tailored to biometric data to those addressing comprehensive consumer data privacy. Over 80 bills have been introduced across 33 states.

Many states that introduced privacy legislation allow for bills to carry over from odd to even-numbered years, meaning that action on these proposals may pick up where it left off. However, as occurred in Virginia and Colorado, new proposals may be better positioned to swiftly move toward passage before policymakers and other stakeholders have time to become entrenched on divisive issues, as we witnessed in Washington in recent years. While privacy legislation has hitherto only been enacted in "blue trifecta" states, many Republican lawmakers have been willing to sign on to similar privacy bills and have been the key drivers of major pushes in states such as Florida, Ohio, and Utah. With even more trifecta states going into 2023, states could be poised to enact data privacy legislation and overcome previous impasses.

In addition to newly introduced legislation, we will see activity in states with existing privacy laws that go into effect in 2023. California and Colorado are in the process of wrapping up rulemaking processes, while Virginia and Connecticut may consider amendments to their newly enacted laws.

Finally, in 2021 the Uniform Law Commission adopted the "Uniform Personal Data Protection Act" which the organization pushed in state legislatures in 2022. While nominally promoting "uniformity," the model law contains several unique elements including a distinction between "compatible", "incompatible" and "prohibited" data practices and provisions for the adoption of "voluntary consensus standards."



Types of Data Privacy Measures

1 Comprehensive consumer data privacy

What:
U.S. Privacy law today consists of various disparate federal and state laws. However, this data privacy framework significantly changed in 2019 with the emergence of the California Consumer Privacy Act, which created a significant compliance burden for most businesses. Since then, activity at the state level has increased as more states look to establish data privacy laws in the absence of a comprehensive federal law. Five states now have comprehensive consumer privacy laws: California (CCPA and its amendment, CPRA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), and Virginia (VCDPA). These laws have similar provisions that typically give consumers some choice in controlling their data.

Where:
- California AB 1490
- Colorado SB 21-190
- Connecticut SB 6
- Utah SB 227
- Virginia HB 2307

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, in which they 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.

2 Biometric

What:
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 the use of biometric data becomes more prevalent, laws like the Illinois Biometric Information Privacy Act (BIPA) are being introduced to prevent private entities. BIPA differentiates biometric data from other personally identifiable information because biometric data cannot be changed readily.

Where:
- Illinois BIPA
- Texas CUBI
- Washington HB 1493
- Maryland SB 335

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

Types of Data Privacy Measures

Children's data privacy / children's safety

What:
Prohibits an operator of an internet website, online service, or mobile application from certain activities when minors are involved. These types of legislation create privacy rights for restricting 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 a growing awareness 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 specified standards or outright ban children from accessing certain platforms.

Where:
- California AB 2273
- West Virginia HB 4325
- Washington HB 1697
- New York S.9563

Impact:
Tech companies appreciate and support the goal to encourage companies to take proactive steps to protect children online. However, these bills would require revisions to decrease subjectivity and provide more guidance on how to comply to avoid requiring organizations to collect more information about children. At a minimum, proposed laws should include cure provisions that allow companies to correct and come into compliance.

Key States To Watch In The 2023 Legislative Cycle

It's expected that legislatures who previously proposed consumer data privacy laws will take up similar efforts.

State	Status
Alaska	Alaska considered HB 159, the Consumer Data Privacy Act. This Act would establish data broker registration requirements, make a violation of the Consumer Data Privacy Act an unfair or deceptive trade practice, and provide for an effective date.
California	In November 2020 the California Privacy Rights Act was enacted by ballot initiative in a 56-43% vote. The law makes significant amendments to the underlying California Consumer Privacy Act and will become effective on January 1, 2023. A newly constituted California Privacy Protection Agency Board engaged in several rulemaking comment periods throughout 2022 and final rules are forthcoming. It is anticipated that there will continue to be future opportunities to engage. California AG Bonta has also been active in urging the Federal Trade Commission "to adopt robust protections against commercial surveillance and data security practices that harm consumers" pointing to California as an exemplar.

Key States To Watch In The 2023 Legislative Cycle

It's expected that legislatures who previously proposed consumer data privacy laws will take up similar efforts.

State	Status
Colorado	The Colorado Privacy Act was enacted in 2021 and directs state Attorney General (AG) rulemaking on the technical specifications for universal opt-out mechanisms. CCIA has been participating in ongoing rulemaking activities throughout 2022. The Colorado Department of Law will hold a final hearing on the proposed rules on Feb.1, 2023 at 10 a.m. MST, and finalized rules must be adopted by July 1, 2023. Governor Polis' signing statement indicates the law will require future "clean-up legislation".
Connecticut	SB 6, An Act Concerning Personal Data Privacy and Online Monitoring was enacted in May 2022 and will become effective on July 1, 2023. The law establishes a framework for controlling and processing personal data, creates privacy protection standards and responsibilities for data controllers and processors, and grants consumers certain rights relating to their data. Throughout Fall 2022, Senator James Maroney (D) has been convening several meetings of the Data Privacy Task Force. The meetings have focused on: algorithmically-informed decision-making; children's privacy protections, including conversations surrounding the UK and CA Age-Appropriate Design Code; data colocation, including whether CT's privacy law should be expanded to include other groups, such as non-profits. We anticipate lawmakers will continue to consider such topics leading into 2023.
District of Columbia	B24-02451, the Uniform Personal Data Protection Act was introduced in October 2021. As introduced, Bill 24-451 would address personal data privacy by establishing information practice principles to the collection and use of personal data from consumers by businesses. The legislation failed to advance.
Florida	In 2021, Florida came close to adopting the Governor DeSantis (R)-endorsed Florida Privacy Protection Act, which passed the State House by a 118-1 vote. The legislation ultimately failed largely because lawmakers in the Senate removed a private right of action provision from their companion legislation. CCIA anticipates that lawmakers will continue to focus on advancing privacy legislation, especially if Governor DeSantis, who has significant popularity in the state, continues to push for such legislation.
Indiana	The Indiana Senate unanimously passed SB 358 concerning consumer data protection, in February 2022. This bill would establish a new article in the Indiana Code concerning consumer data protection, to take effect January 1, 2025. Prior to its passage in the Senate, the bill was amended to more closely reflect the provisions of the Virginia Consumer Data Protection Act. The Senate-passed version removed language allowing for a private right of action, and does not require controllers to recognize universal opt out signals and does not grant the Indiana Attorney General rulemaking authority.

Key States To Watch In The 2023 Legislative Cycle

It's expected that legislatures who previously proposed consumer data privacy laws will take up similar efforts.

State	Status
Iowa	The Iowa House amended and passed H.F. 2506 on a 91-2-7 vote on March 15, 2022. By state law, the Iowa Senate needed to pass the bill out of committee by March 18, 2022 despite the fact that the legislature did not adjourn until later in the spring. The bill would largely mirror the provisions found in Utah's consumer data privacy law. Given the strength of support for this proposal this past legislative session, we expect similar proposals to resurface and gain momentum next year.
Maryland	The Maryland General Assembly enacted HB0962/SB0643, which became effective on October 1, 2022, and amended the Maryland Personal Information Protection Act. The amendments update and clarify aspects of the Act, including the timeframe for reporting a data breach and requirements for providing notice to the Maryland AG. CCIA is expecting that Maryland will tackle broader consumer data privacy protection in 2023, potentially in the form of a working group.
Massachusetts	The Massachusetts House considered H. 4514, the Massachusetts Information Privacy and Security Act, and while this bill was reported out of the Committee on Advanced Information Technology, the Internet and Cybersecurity, the Joint Committee on Health Care Financing sent the bill to "study", which in Massachusetts means that the bill will not be further reviewed by the committee.
Missouri	The Missouri House passed HB 212, the Personal Privacy Protection Act in March 2022, and while the Senate voted to pass the measure, it did not advance for a floor vote. The bill would prohibit public agencies from disclosing or requiring disclosure of personal info.
New Jersey	A. 505, The New Jersey Disclosure and Accountability Transparency Act was referred to the Science, Innovation and Technology Committee in January 2022. It establishes certain requirements for disclosure, processing of personally identifiable information, and an Office of Data Protection and Responsible Use in the Division of Consumer Affairs. S.332 was referred to the Senate Commerce Committee in January 2022, reported from the Senate Committee in June 2022, and went through Senate Amendments in August 2022. This bill requires commercial websites and online services to notify consumers of collection and disclosure of personally identifiable info and allows consumers to opt out. The New Jersey legislature uniquely carries over legislation between even- to odd-numbered years, so any pending measures will still be up for consideration leading into 2023. It is also worth noting that New Jersey hold "off-cycle" elections when compared to its other state counterparts. The looming elections in Fall 2023 may impact the prospects of more "controversial" legislative measures making it across the finish line.

Key States To Watch In The 2023 Legislative Cycle

It's expected that legislatures who previously proposed consumer data privacy laws will take up similar efforts.

State	Status
New York	Numerous sweeping privacy bills were introduced in New York this session. Most significantly, initial versions of the (former) Governor's budget included the "New York Data Accountability and Transparency Act." Senator Thomas, Chair of the Consumer Protection Committee also re-introduced the "New York Privacy Act" which includes quasi-fiduciary duties of "care" "loyalty" and "confidentiality." S6701B, which relates to enacting the New York Privacy Act, is currently in the Internet And Technology Senate Committee. Given the flurry of privacy-related legislation in recent New York legislative sessions, it is almost certain these conversations will continue in 2023.
Pennsylvania	HB 2257, The Consumer Data Protection Act was referred to the Consumer Affairs House Committee in January 2022, but failed to further advance. This bill would provide protection of consumer personal data, impose duties on controllers and processors of personal data, provide for enforcement, prescribe penalties, and would establish the Consumer Privacy Fund.