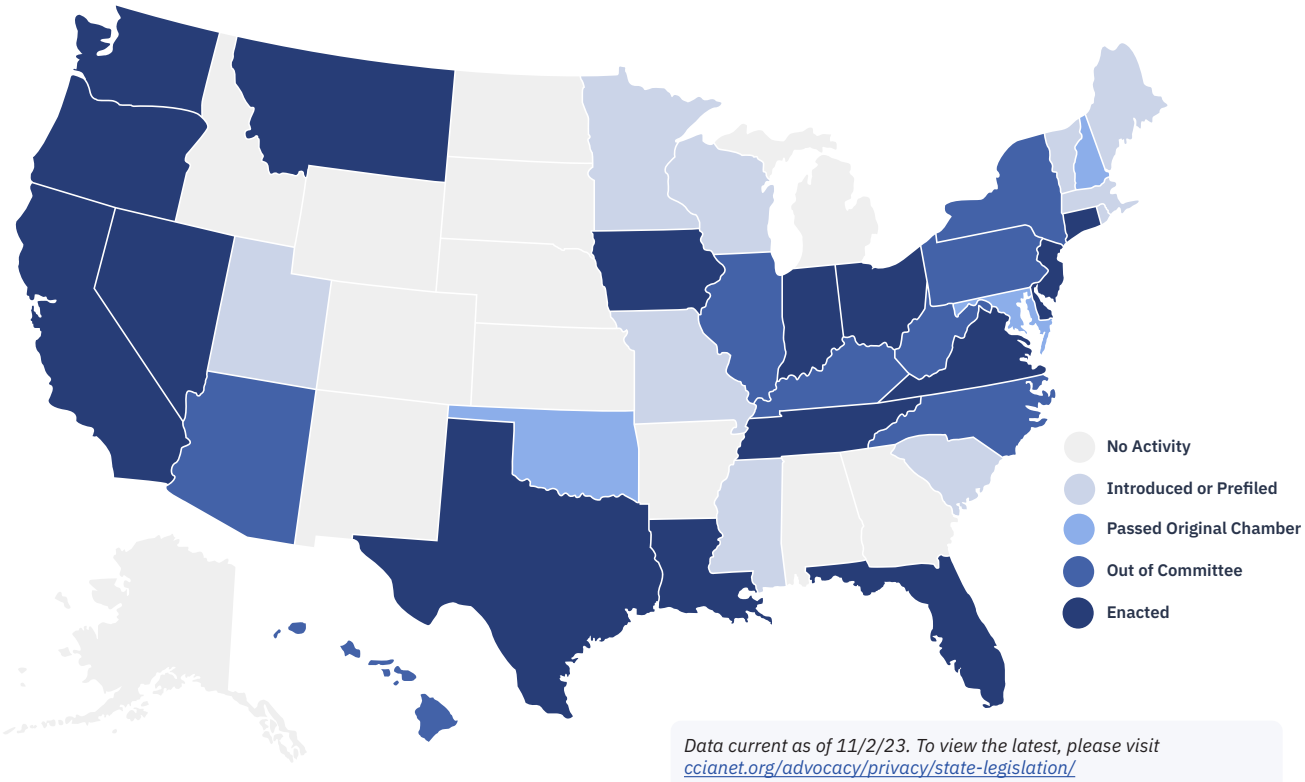
Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.org

State Landscape
Privacy

2023 State Landscapes



Data current as of 11/2/23. To view the latest, please visit ccianet.org/advocacy/privacy/state-legislation/

Introduction

In the backdrop of the continuing impasse on federal privacy legislation, states continued to introduce measures aimed at addressing an array of data privacy concerns – ranging from bills tailored to biometric or health data to those addressing comprehensive consumer data privacy. In 2023 alone, the first year of the biennium for many state legislatures, over 140 bills have been introduced across 37 states. Just last year, CCIA reported that over 80 bills had been introduced across 33 states, marking a significant increase – it is almost certain that policy debates about data privacy will continue across the 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 Maryland in recent years. Prior to 2023, comprehensive consumer privacy legislation had largely been a phenomenon enacted in "blue trifecta" states, with Utah being the primary exception. However, 2023 ushered in a "red wave" of states enacting such laws – Indiana, Iowa, Montana, Tennessee, and Texas joined California, Colorado, Connecticut, Utah, and Virginia is establishing comprehensive consumer data privacy laws, while Democrats in Delaware, Oregon, and Washington led the charge to pass legislation as well. In 2024, it is anticipated that those states who considered and "carried over" legislation from the first year of the biennium will continue debating such proposals while even more states will follow suit in introducing their own frameworks.

In 2023, California and Colorado released guidance following two lengthy rulemaking processes and by the end of the calendar year laws in Colorado, Connecticut, and Virginia will have become effective. And in 2024, California Privacy Rights Act regulations will go into effect along with the recently enacted laws in Florida, Montana, Oregon, Texas, and Washington. In addition to comprehensive data privacy laws, it is likely that states on both sides of the aisle will continue considering proposals related to biometric and health data in addition to privacy protections specifically targeted to younger users. Below, CCIA offers details regarding state-level data privacy conversations during the 2023 session along with a look-ahead to the 2024 legislative sessions.

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 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. Twelve states have now enacted comprehensive consumer data privacy laws – California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia. Florida also passed data privacy legislation in 2023, however, the law is tailored to focus on a narrower set of businesses in the technology and digital services sector.

Where:

- ME L.D. 1977
- MD SB 698
- VT H. 121
- WI AB 466

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 Information / Health 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 the use of 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.

Where:

- MA S. 184/H.386
- NV SB 370
- NY S. 365/A. 7423
- WA HB 1155

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.

3 Data Protections for Younger Users

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 vague standards or outright ban children from accessing certain platforms.

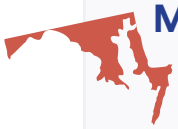
Where:

- CT SB 3
- VA HB 1688/SB 1026

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, provide more guidance on how to comply to avoid requiring organizations to collect more information about children, and avoid restricting the use of tools like tools and systems 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



Maryland

The Maryland General Assembly continued data privacy concerns from the 2022 legislative session in earnest during 2023. These conversations spanned the consideration of a comprehensive consumer data privacy bill that also included proposed protections for biometric data in addition to specific proposals modeled after the California AADC. While there was substantive debate and consideration of all these proposals none were enacted but it is almost certain that similar conversations will continue in 2024.

Massachusetts

The Massachusetts Legislature has considered several bills that aim to provide privacy protections for consumer health data, as well as data related to geolocation. These bills have received a hearing in June in the Consumer Protection Committee but have not yet moved forward in the legislative process since then. Massachusetts' Legislature is typically more active in its second session year and given the large number of co-sponsors for these bills, there is a strong possibility that further action will be taken in 2024.

Maine

The Maine Legislature considered several different consumer data privacy bills in 2023, including two different comprehensive data privacy bills as well as data privacy bills specific to health data and another related biometric data. The Legislature did not move forward with any one particular proposal but the Judiciary Committee has been conducting work sessions on the topic to decide which avenue they want to take up in 2024.

Key States

Michigan

In recent years, Michigan has considered but not successfully passed a comprehensive consumer data privacy law. However, it is likely that lawmakers will introduce and consider another proposal before the biennium concludes in December 2024. As a full-time legislature, Michigan lawmakers meet year-round and legislation carries over from odd year to even, meaning measures from 2023 are eligible for consideration in 2024 as well.

New York

The New York Senate passed a comprehensive data privacy bill in the final weeks of their legislative session. The Assembly's companion bill was not introduced until late in the session and ultimately was not taken up. The bill will now restart the legislative process in 2024, with a notable update - the primary Senate bill sponsor, Kevin Thomas, is running for Congress, so there is potential of him trying to push his bill to support his campaign effort.

Vermont

Vermont's House Commerce Committee considered a comprehensive data privacy bill that was being pushed by the Attorney General's office. After several hearings and deliberations, the Committee decided not to move forward with the bill in its current state and instead is planning on crafting a comprehensive data privacy bill that is more similar to Connecticut's data privacy law and introducing that bill in 2024.

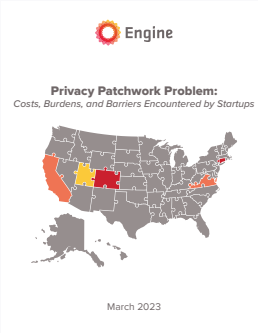
Wisconsin

Unlike many other state legislatures, Wisconsin lawmakers meet year-round and are currently considering a comprehensive consumer data privacy framework. As introduced, the proposal largely mirrors the definitions and business obligations outlined in other state frameworks, and also similar to all other states who have enacted data privacy laws, does not allow for a private right of action. If lawmakers do not pass the measure before the end of the 2023 calendar year, it will carry over to the 2024 legislative session.

Wyoming

While the Wyoming legislature has yet to formally introduce a comprehensive consumer data privacy framework, lawmakers have started conversations during the interim period. In May, the state's Select Committee on Blockchain, Financial Technology and Digital Innovation Technology convened a meeting to discuss a draft privacy bill outline signaling that state lawmakers are poised to take up formal conversations on this topic in the near future.

Collected Analysis

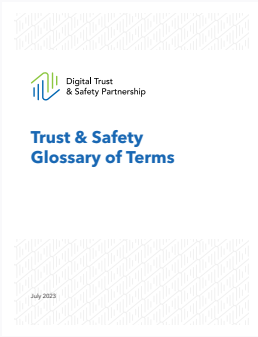


Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startup

Engine

Engine published a report Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startups that details the unique challenges that startups face in light of the growing patchwork of state privacy laws and the lack of a national privacy standard at the federal level. The report highlights that a patchwork risks preventing startup growth as compliance costs could add additional burdens to businesses that are already resource-strapped.

This report is available at: https://www.engine.is/news/category/engine-releases-report-on-privacy-patchwork-problem-costs-burdens-and-barriers-encountered-by-startups

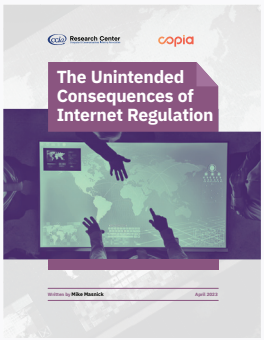


Trust & Safety Glossary of Terms

Digital Trust & Safety Partnership

The Digital Trust & Safety Partnership (DTSP) released the inaugural edition of its Trust & Safety Glossary of Terms. This is the first industry effort by technology companies, representing various products, sizes, and business models, to develop a common Trust and Safety lexicon. The glossary has been updated to incorporate valuable input received from academic organizations, industry partners, regulators, and other global stakeholders during the public consultation held earlier this year.

This report is available at: https://dtspartnership.org/wp-content/uploads/2023/07/DTSP_Trust-Safety-Glossary_July-2023.pdf



The Unintended Consequences of Internet Regulation

The Copia Institute & CCIA Research Center

The Copia Institute & CCIA Research Center released a report examining unintended consequences of internet regulation, including the poor targeting of many of these policies, the slowing of investment in online businesses, and the inability of smaller start-up firms to compete.

This report is available at: https://research.ccianet.org/reports/unintended-consequences-of-internet-regulation/