A Comparison of States' Governance Requirements Concerning Citizens' Personal Data

Anatoliy Lawrence
Research Assistant
Idaho State University

Joshua Kyle Lindquist
Research Assistant
Idaho State University

Noah Passey
Research Assistant
Brigham Young University

October 2025

UVU GARY R. HERBERT INSTITUTE *for* PUBLIC POLICY
800 W University Pkwy, Orem, UT 84058
801-558-9371 | uvu.edu/herbertinstitute/

Introduction

As of July 2025, nineteen US states have enacted consumer data privacy laws.[1] These laws began with the 2018 California Consumer Privacy Act (CCPA), and as consumer laws, they apply only to businesses and how they handle consumers' personal data.[2] In contrast, government-focused data governance laws regulate how government entities collect and use personal data and enforce transparency requirements and privacy standards. The federal government has never developed a data privacy law that applies to state or local entities. The most prominent federal law in this area—the Privacy Act of 1974—governs only the federal government's data management.[3] In the absence of federal standards, states have begun to self-regulate their data governance practices. Currently, there are six states with comprehensive legislation that applies to government privacy.[4]

Government entities inherently collect and process large amounts of very sensitive data. In the absence of relevant legislation, this data collection can result in mass profiling, misuse, unregulated sharing, and surveillance.[5] Outside of this research, there is no current public documentation that tracks the status of US government privacy law.

Data Governance vs. Data Privacy

Government privacy is something that overlaps with the concept of data governance. As defined by the Herbert Institute for Public Policy, "Data governance is the framework of laws, rules, policies, practices, and procedures that ensure effective management, privacy, and transparency of data collected by governmental entities."[6] Privacy is just one component of the broader concept of data governance. Specifically, privacy as defined by the National Institute of Standards and Technology is "freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual."[7]

This paper addresses the current climate of US state laws and policies in several different data governance concepts—transparency, privacy, and use. It does so by identifying a total of twenty-nine different practices that would be mandated in an ideal government privacy law. This paper divides these twenty-nine practices into eight governance principles and searches for these principles and practices in state law and state policy (i.e. administrative code, executive orders).

Law vs. Policy

In the United States, legislation carries greater authority and durability than other forms of rulemaking or policy. Laws are legally binding, centrally enacted through formal processes, and enforceable through fines, civil penalties, or criminal sanctions. In contrast, policies—particularly those issued at the agency or administrative level—are generally not as enforceable in a court of law. They are more susceptible to change, often shifting with political leadership or administrative priorities. While compliance with state-level policies may be a condition for funding or intergovernmental cooperation, such policies generally do not carry the same legal force as statute.

Methodology

The following sections outline each of the eight governance principles and their associated practices, which together form the basis for analyzing current state laws and policies. This paper pulls data from every state's publicly available laws and policies and evaluates them to see if they met the practices in each section.[8] It uses the International Association of Privacy Professionals (IAPP) Comprehensive Consumer Privacy Bills chart and adapts the concept for government entities. This paper adds in sections that are relevant to government data privacy—principles like transparency, purpose-use limitations, and compliance.[9]

Core Principles and Practices

Comprehensive Law

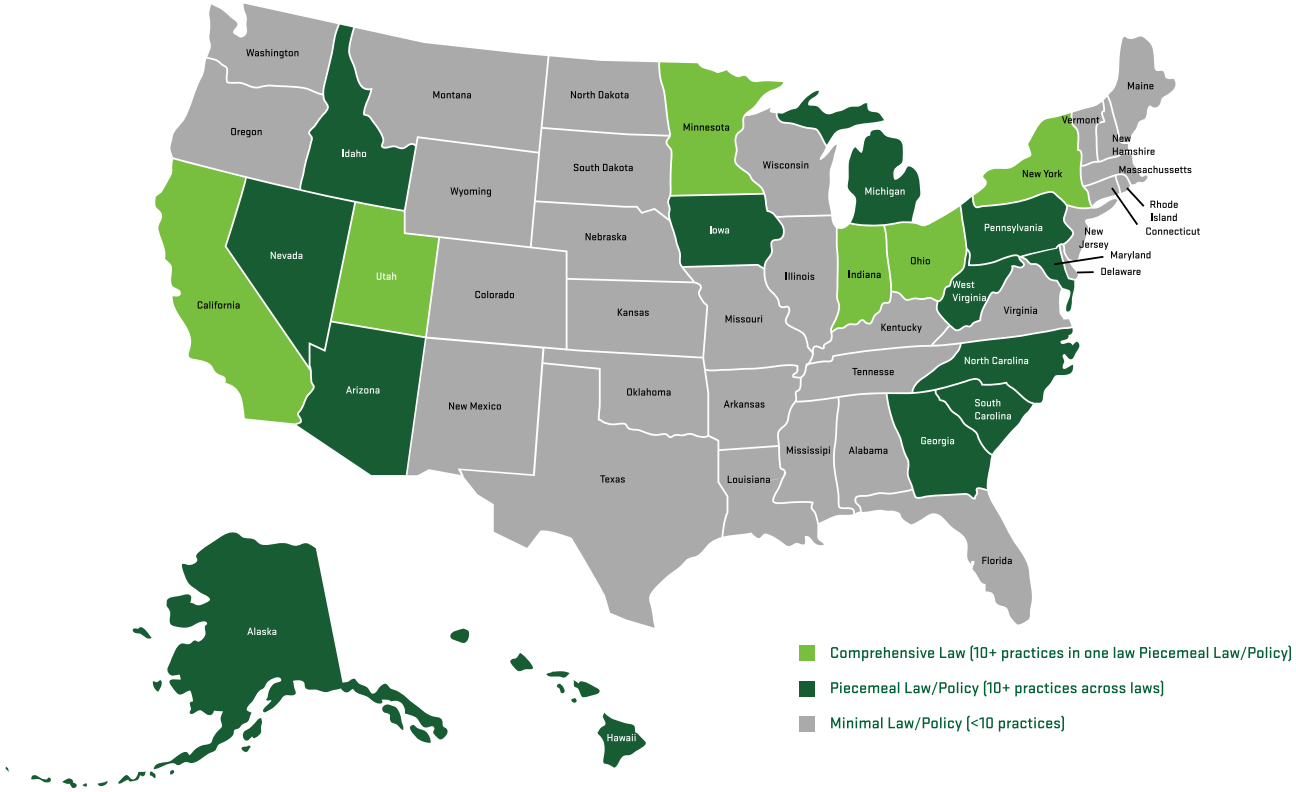
The ideal state privacy legislation is collected together in one comprehensive law. The International Association of Privacy Professionals (IAPP) describes a privacy law as "narrow in scope if it applies only to a specific set of data types . . . [or] if it is targeted at providing only one or two . . . data rights, such as deletion or correction."[10] A comprehensive law, on the other hand, applies to several different data types and provides data rights in multiple areas.

For the purposes of this paper, a comprehensive privacy law is one that meets ten or more of the identified twenty-nine practices. Most states have some legislation that limits how government entities collect and use data,[11] but these limitations are typically spread out over different statutes across their state code—a form of piecemeal law or policy.

A comprehensive data privacy law is preferable because it leads to greater transparency, accountability, and compliance. Transparency increases with a comprehensive law because a centralized bill makes it easier for citizens to understand how governmental entities handle their data. They are then able to hold their officials accountable to these standards. Compliance is also more likely because government officials have a single cohesive source of instructions for how to handle citizens' data. Furthermore, the enactment of a comprehensive data privacy law affirms that data privacy is not merely a byproduct of broader legislative efforts,

Fig. 1. State Data Governance Legislation and Policy

What level of legislative maturity do states have regarding data governance?



but a distinct and deliberate policy priority in its own right.

The states that currently have a comprehensive government privacy law are

- California—Information Practices Act of 1977
- Indiana—Fair Information Practices
- Minnesota—Government Data Practices Act
- Ohio—Personal Information Systems
- Utah—Government Data Privacy Act

The laws in California, Ohio, Indiana, and Minnesota all began decades ago,[12] each with recent amendments that help these following principles apply to the digital age. West Virginia and Pennsylvania are unique in that they have, respectively, an executive order and an authorized privacy policy that each cover most privacy principles without having the authority of law.[13] Seventeen other states have legislation or policy that address significant aspects of data governance and privacy; these are just spread out through different laws and policies.[14]

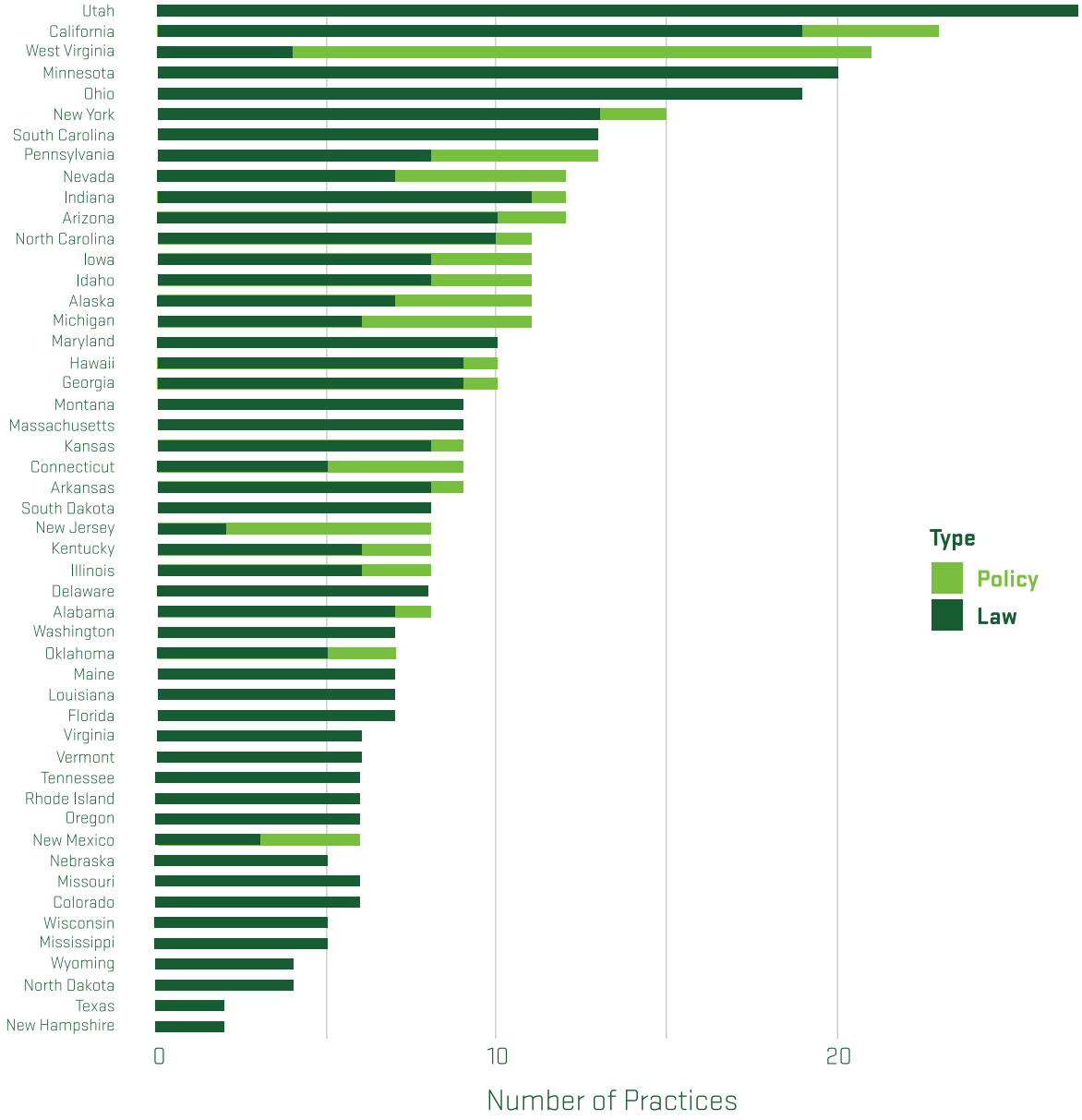
Records management/control

Records management is the process of identifying, cataloging, organizing, and disposing of information so that it is accessible and protected. Records management controls include practices like establishing a records governing body, requiring appointed records officers, enacting protection for records involving at-risk government employees, and establishing processes for citizens to correct their own data. Records management is critical for accountability of government actions.[15]

The vast majority of states do have legal requirements that govern records management.[16] Records officers are a well-established part of most bureaucracies, as are archival systems. Processes for correcting data or protecting certain employees' data are less common, however. Most states simply create an organization with the authority to manage and maintain records and assign various individuals as liaisons with that organization. Their focus is less on privacy and more on maintaining information for future use.[17]

Fig. 2. Number of Practices Required by State

How many of the 29 practices are required by law or policy?



Access to records

Record access involves limiting who sees and uses the data in an entity's records management program. Requirements in this category include whether entities are required to classify data, whether an individual has the right to access their own data collected by the state, and what limitations are in place as to who can access those records. This last one is essential; without proper limitations in place, government employees may have access to any personal data collected by the state.[18]

In consumer privacy laws, the vast majority of bills include provisions on accessing one's own data. This is not true for government data privacy—less than a third of states mandate this practice. Many states do have some sort of limitations on who can access confidential or private information, however, and the vast majority are required to classify records as public or private. Some states, like Connecticut, have even more explicit classification requirements that involve more levels of security and privacy, such as labeling levels of potential impact and confidentiality like.[20]

Data privacy roles and responsibilities

Data privacy roles and responsibilities are less focused on general data governance and more on the specifics of privacy. In order to satisfy these requirements, a state must have laws mandating the existence of privacy officers within entities and the construction of a statewide privacy oversight body. It must also mandate that entities implement data governance/privacy training, complete regular privacy impact/risk assessments, and identify high-risk processing activities such as third-party sharing or large-scale integration.[21]

Few states have statutory requirements in this category. Some states do require that privacy officers are designated within certain entities, but very few fulfill any of the other requirements. Utah's Government Data Privacy Act (GDPA) does mandate these practices, and West Virginia's Privacy Policy (authorized by Executive Order No. 6-06) requires four out of the five.[22] This is only in declared policy, however, and does not have the longevity or enforceability of law (see Fig. 2).

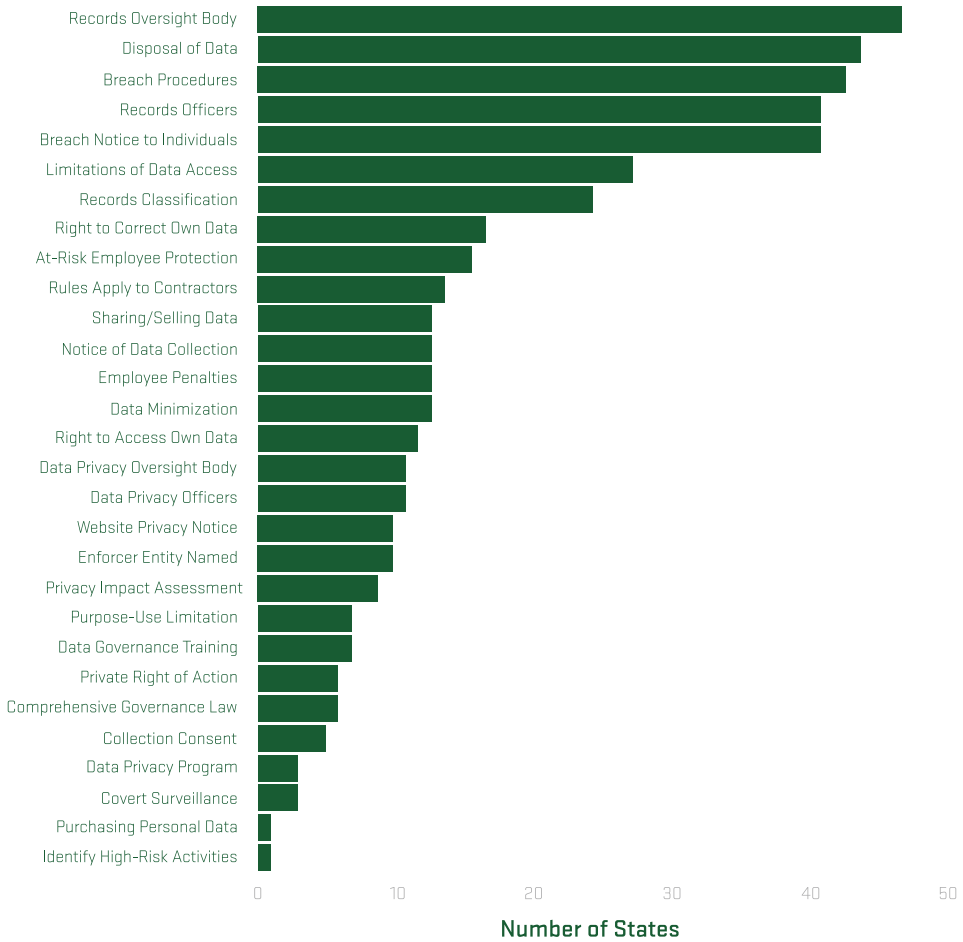
Transparency

Government entities sometimes collect and process information in ways that the public isn't aware of.[23,24] Transparency requirements ensure that entities only collect and process data in ways that are clearly explained to the public. This includes a notice of data collection at the time of collection, website privacy notices on all webpages and especially where technology like cookies are relevant, and a regular privacy report that keeps government privacy and security efforts accountable to the public.[25]

Transparency is a topic that is not often covered in any state legislation. Several states have scattered requirements for providing notice at the time of data collection,[26] and several others cover these practices with various declared policies that do not have the force of law.[27] Utah and California are the only states to require all three of these things in law,[28] and California does so through a combination of multiple disparate laws.[29]

Fig. 3: Number of Sates per Practice

How many states require this?



Purpose-use limitations

Purpose-use limitations limit how much data governmental entities collect as well as how they use that data. Data privacy requires that entities collect the minimum amount of data necessary to perform their assigned functions, a concept called data minimization. Purpose-use limitation requires that entities have a clear purpose for the data they collect, that they state that purpose to citizens at the time of collection, and that they limit their use of that data to those specific purposes. Using citizens' data for research or other activities means violating this requirement.[30]

Entities sometimes share citizen data between departments or even sell it, and this isn't always done with citizens' consent or within their stated purposes.[31] An ideal data governance law has explicit requirements in place for the sharing and selling of data as well as the purchasing of data.[32] Few states have any of these requirements, and there is only one that mentions data purchasing.[33] Montana SB 282 expands rights regarding illegal searches and seizures to apply to digital data, specifying that personal data cannot be purchased without a warrant or subpoena.[34]

Security measures

Data governance and data privacy both include data security. Data security refers to the technical and procedural measures used to protect data from unauthorized access.[35] The practices in this principle include whether entities are required to dispose of personal data when it is no longer necessary, whether entities are required to notify citizens of data breaches involving their data, and whether there are consistent procedures in place for responding to and recovering from a data breach. The final practice also identifies whether these requirements extend to government contractors or whether they are limited to entities themselves as the data controllers.[36]

The vast majority of states have some form of data breach law requiring citizens to be notified if their personal data was involved in some form of breach.[37] Most states also mention destroying/disposing of records when they are no longer of use, although statutory language is often unclear.[38] Many states mention that data may be destroyed or lay out the limitations on record disposal.[39] Only five states have language that explicitly mandates the destruction of such records—Florida, Montana, Nevada, New Hampshire, and Utah.[40]

Compliance

While many states lack comprehensive government data privacy legislation making full compliance with privacy standards challenging, some states have taken steps to establish basic compliance frameworks.[41] Among those with explicit privacy policies or laws, a number have designated enforcement authorities and outlined penalties for violations.[42] Thirteen states, for example, specify particular sanctions related to data breaches or other privacy infractions.[43] Additionally, a few states, including Hawaii and Arkansas, elevate certain privacy violations to the level of criminal offenses, underscoring the seriousness with which these issues are treated.[44] Despite these advances, significant gaps remain in ensuring consistent enforcement and providing citizens with mechanisms, such as private rights of action,[45] to hold governments accountable.

Trends

There are several significant trends visible from this data. First, as shown in Fig. 1, there are very few states with a comprehensive privacy law.[46] Most states either have a collection of disconnected laws that cover the relevant requirements, or they barely have any laws that mention privacy concepts.[47] Fig. 2 shows the number of practices covered by each state's policy and legislation.[48] This paper tracks twenty-nine practices, and only ten out of fifty states covered 50% of the practices–in law or in policy.[49]

These data show that certain privacy concepts are much better defined and better covered by state laws than others. As mentioned above, records management concepts and breach procedures are present in almost every state's laws.[50] Laws and policies that relate directly to privacy are less common,[51] and very few states have specific requirements like those that explicitly prevent covert surveillance or the purchasing of personal data from third parties.[52]

Conclusions

While many states have drafted and passed legislation surrounding consumer data privacy, very few have done the same for government data privacy. Certain principles from data governance and data security have been slowly adopted across the US, giving citizens' privacy some indirect protections. However, most privacy protections are incomplete, difficult to comply with, or missing entirely. A comprehensive data privacy law is one of the clearest ways to address this gap, modernize antiquated record requirements, and prioritize citizen's interests. Today, citizens of different states have very different rights regarding their privacy. Minimizing those differences and making privacy a priority in government agendas will likely require significant legislative change.

Bibliography

1. IAPP. U.S. State Privacy Legislation Tracker 2025. July 7, 2025. Accessed August 7, 2025. https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf
2. California Legislative Information. California Consumer Privacy Act of 2018. California Civil Code § 1798.100-1798.199. Accessed August 7, 2025. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
3. Privacy Act, 5 U.S.C. § 552. Accessed August 7, 2025. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title5-section552&num=0&edition=prelim
4. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
5. Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York: Picador, 2018)
6. Freedman, William, Grace Wingate, Barclay Burns, and David R Connelly. "The Current State of Data Governance in Utah." February 2025. Accessed August 7, 2025. https://www.uvu.edu/herbertinstitute/docs/web_the_current_state_of_data_governance_in_utah.pdf
7. National Institute of Standards and Technology. "Privacy." NIST Computer Security Resource Center. Accessed August 7, 2025. https://csrc.nist.gov/glossary/term/privacy
8. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
9. IAPP. U.S. State Privacy Legislation Tracker 2025. July 7, 2025. Accessed August 7, 2025. https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf
10. Folks, Andrew. "Defining 'comprehensive': Florida, Washington and the scope of state tracking." IAPP, February 22, 2024. Accessed August 7, 2025. http://iapp.org/news/a/defining-comprehensive-florida-washington-and-the-scope-of-state-tracking/
11. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
12. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
13. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
14. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
15. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
16. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
17. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
18. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
19. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
20. State of Connecticut, Office of Policy and Management, "Data Classification Methodology," December 5, 2019, accessed August 11, 2025, https://portal.ct.gov/-/media/opm/fin-general/dataclassificationmethodology120519pdf.pdf?rev=81120310428448d9a44420e829d4a005&hash=-3F9555EAAD35BE9474E09EEAD10F82BA.
21. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
22. Utah State Legislature, "Utah Code, Title 63A, Chapter 19," PDF, May 1, 2024, accessed August 11, 2025, https://le.utah.gov/xcode/Title63A/Chapter19/C63A-19_2024050120240501.pdf; West Virginia Board of Risk and Insurance Management, "West Virginia Executive Branch Privacy Policies," last modified 2009, accessed August 11, 2025, https://privacy.wv.gov/SiteCollectionDocuments/Privacy%20Policies/Privacy%20Policy%20Issuance%20WVEB-P100.pdf.
23. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
24. Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York: Picador, 2018). Evelyn Ruppert, "Doing the Transparent State: Open Government Data as Performance Indicators," in The World of Indicators: The Making of Our Global Knowledge, ed. Richard Rottenburg, Sally E. Merry, Sung-Joon Park, and Johanna Mugler (Cambridge: Cambridge University Press, 2015)
25. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
26. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
27. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
28. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.

29. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
30. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
31. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
32. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
33. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
34. Montana State Legislature, SB 252, 2025 Leg. Sess. "AN ACT GENERALLY REVISING SEARCH AND SEIZURE LAWS RELATED TO THE ABILITY OF THE STATE AND LOCAL GOVERNMENT TO OBTAIN AND USE ELECTRONIC COMMUNICATIONS AND RELATED MATERIAL AND STORED DATA OF AN ELECTRONIC DEVICE...", last updated May 8, 2025, accessed August 11, 2025, https://bills.legmt.gov/#/laws/bill/2/LC0061?open_tab=bill.
35. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
36. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
37. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
38. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
39. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
40. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
41. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
42. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
43. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
44. Haw. Rev. Stat. § 92F-17, 2024, accessed August 12, 2025; Ark. Code § 25-19-104, 2024, accessed August 12, 2025.
45. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
46. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
47. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
48. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
49. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
50. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
51. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.
52. Utah Office of Data Privacy. US State Data Governance Law Tracker. Version 1.2. August 27, 2025. Accessed October 21, 2025.