ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

The State of Privacy: Lessons From State Laws for a National Framework

ASH JOHNSON I JUNE 2026

The United States' patchwork approach to privacy is unworkable in the long term. But that patchwork is already here, and Congress can learn from the policies states have implemented to craft a national data privacy framework.

KEY TAKEAWAYS

- Meaningful differences have emerged in how state privacy laws define key terms, allocate rights to consumers, impose obligations on data holders, and structure oversight and enforcement.
- The vast majority of broad state privacy laws share common provisions that could provide Congress with a useful starting point when crafting federal legislation.
- There are more significant areas of consensus between state privacy laws than there are significant areas of contention, including key definitions, consumer rights, data holder responsibilities, and enforcement mechanisms.
- There are two main areas of contention among state privacy laws: the inclusion of a universal opt-out mechanism and whether a law's opportunity to cure is guaranteed or discretionary.
- The state privacy patchwork is both expensive for businesses and confusing for consumers. Congress should act quickly to pass a federal privacy law that establishes a uniform national standard by preempting all state privacy laws.

CONTENTS

INTRODUCTION

The rapid proliferation of broad state data privacy laws across the United States has created a complex and fragmented regulatory landscape. While these laws share common goals of enhancing consumer rights, increasing transparency, and imposing obligations on data holders, they diverge in key definitions, scope, enforcement mechanisms, and substantive requirements. This patchwork approach presents significant challenges for both consumers and businesses. Individuals face inconsistent protections depending on where they live, while companies—particularly those operating across state lines—must navigate a maze of overlapping and sometimes conflicting obligations. The result is increased compliance costs, legal uncertainty, and uneven privacy outcomes nationwide.

These challenges underscore the growing need for a national data privacy framework. A federal standard would provide consistent baseline protections for all Americans, regardless of geography, while simplifying compliance for businesses and fostering innovation. The longer Congress waits to accomplish this goal, the greater the risk of further entrenching fragmentation as more states enact their own laws, potentially amplifying inconsistencies and complicating enforcement. A well-designed federal law would strike a balance between protecting consumers, enabling responsible data use, and ensuring regulatory clarity.

The United States' patchwork approach to privacy is unworkable in the long term. But that patchwork is already here, so at the very least, Congress can learn from the policies states have implemented, systematically comparing these laws to identify best practices and avoid pitfalls.

This report compares and contrasts the existing 21 broad state data privacy laws to inform Congress's efforts to craft a national data privacy framework. It breaks these laws down into their core provisions, including key definitions, consumer rights, data holders' responsibilities, and oversight and enforcement mechanisms, highlighting areas of significant overlap and noteworthy differences. It then analyzes these similarities and differences based on their proven or estimated impact on consumers, businesses, and the economy. Finally, the report recommends which provisions from state privacy laws Congress should draw from in constructing a federal data privacy framework.

Table 1: Summary of recommendations on 10 key aspects of a federal data privacy law

Recommendation	Reasoning
Exclude anonymous and de-identified data from the definition of personal data.	This would enable greater innovation using nonsensitive forms of data.
Limit the definition of sensitive data to categories of personal data that have the greatest potential to cause financial, physical, or reputational harm.	This would target the most likely causes of privacy-related harm.
Give consumers the right to opt out of personal data collection and sharing or profiling for significant decisions and require businesses to obtain affirmative consent for sensitive data.	This would balance the interests of protecting consumers, giving consumers greater control and enabling innovation through data.
Require businesses to conduct risk assessments only before processing personal data that poses a "heightened risk" to consumers.	This would minimize the compliance burden on businesses while still protecting consumers from real privacy harms.
Require businesses to implement reasonable security practices but avoid specific, prescriptive cybersecurity requirements.	This would protect consumers' personal data and give businesses the flexibility they need to adapt to different levels of cyberrisks and attackers' ever-evolving methods.
Require businesses to provide accessible privacy notices and conspicuous opt-out disclosures but avoid specific instructions on how businesses should design these notices and disclosures.	This would provide greater transparency to consumers without inconveniencing businesses or consumers.
Omit data minimization or purpose specification and limitation requirements.	This would avoid placing limits on innovation and flexibility that ultimately benefit consumers.
Omit a private right of action.	This would avoid unnecessarily exposing companies to substantial legal costs due to meritless lawsuits.
Omit a universal opt-out mechanism.	This would protect ad-supported businesses that provide services to consumers at a low or no cost.
Include a guaranteed opportunity to cure.	This would incentivize businesses to comply in good faith and correct mistakes while still leaving room for regulators to punish bad actors.

DIGGING INTO THE STATE PRIVACY PATCHWORK

As the United States continues to develop a patchwork of broad state privacy laws, meaningful differences have emerged in how states define key terms, allocate rights to consumers, impose obligations on data holders, and structure oversight and enforcement. While many of these laws share a common foundation—drawing heavily from early models such as California's or Virginia's framework—they diverge in critical ways that shape both their practical impact and compliance burdens.

This section looks at four core areas of divergence across state privacy regimes: key definitions that determine scope and applicability, the breadth of consumer rights, the substantive responsibilities imposed on businesses, and the mechanisms for oversight and enforcement. While there are many other provisions contained in the 21 broad state privacy laws that differ from state to state, these four areas not only encompass the provisions that have the greatest impact on businesses and consumers, but also highlight where states have converged toward common standards and where fragmentation persists.

Key Definitions

Key definitions contained within state privacy laws determine whom the law applies to. State laws also define different categories of data. These laws typically include protections for "personal data" (also referred to as "personal information" or "personally identifiable information") and increased protections for "sensitive data" (also referred to as "sensitive information").

Though there is some slight variation, generally speaking, state privacy laws apply to firms conducting business in a state or targeting their products and services to a state's residents. These businesses must also meet certain thresholds, typically determined by the number of consumers whose data the business processes each year or the percentage of the business's annual revenue derived from data sales. In California, businesses that meet a certain minimum threshold of annual revenue must also comply with the state's privacy law regardless of the volume of data they process or the percentage of revenue they derive from data sales. In Tennessee and Utah, businesses must meet a certain minimum threshold of annual revenue in addition to processing volume or data sale minimums. Three states—Minnesota, Nebraska, and Texas—approach size-based restrictions in a different way, exempting small businesses, as defined by the U.S. Small Business Administration.

As the United States continues to develop a patchwork of broad state privacy laws, meaningful differences have emerged in how states define key terms, allocate rights to consumers, impose obligations on data holders, and structure oversight and enforcement.

Notably, Florida's privacy law only applies to very large companies—those making over $1 billion in gross annual revenue.[1] Because this definition only includes a small percentage of businesses that process or sell consumer data, this report does not include Florida's law under its definition of "broad state data privacy laws."

The most common definition of personal data is "information that is linked or reasonably linkable to an identified or identifiable individual." Nineteen states use this definition. California's

definition is substantively different and broader: "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a consumer or household."[2] Tennessee uses a similar definition. All 21 broad state privacy laws exclude de-identified or publicly available data from their definitions of "data."

Definitions of sensitive data typically include information that reveals an individual's race or ethnicity, religious beliefs, mental or physical health conditions or diagnoses, sex life or sexual orientation, or citizenship or immigration status. Sensitive data also typically includes uniquely identifying genetic or biometric data, personal data from a known child, and precise geolocation data. Delaware, Maryland, New Jersey, Oregon, and Utah each have additional categories of sensitive information, but their definitions mostly align with the standard definition. California's definition is by far the most expansive, with unique categories including social security, driver's license, state ID card, or passport numbers; financial information; credentials allowing access to an account; philosophical beliefs; union membership; neural data; consumer health data; and contents of mail, email, text messages, or all three.

Table 2: Key definitions in state privacy laws

State	Applicability	Personal Data	Sensitive Data
Alabama[3]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
California[4]	▪ Entities conducting business in the state ▪ Includes a minimum threshold determined by annual revenue, volume of processing, or sale of data	▪ Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a consumer or household ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive ▪ Social security, driver's license, state ID card, or passport numbers ▪ Financial information ▪ Credentials allowing access to an account ▪ Philosophical beliefs ▪ Union membership ▪ Genetic or neural data ▪ Consumer health data ▪ Contents of mail, email, or text messages

State	Applicability	Personal Data	Sensitive Data
Colorado[5]	▪ Entities conducting business in the state or producing or delivering commercial products or services intentionally targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
Connecticut[6]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
Delaware[7]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive ▪ Pregnancy ▪ Status as transgender or nonbinary ▪ National origin ▪ Genetic or biometric data
Indiana[8]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive

State	Applicability	Personal Data	Sensitive Data
Iowa[9]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
Kentucky[10]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
Maryland[11]	▪ Entities conducting business in the state or providing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive ▪ Consumer health data ▪ Status as transgender or nonbinary ▪ National origin ▪ Genetic or biometric data
Minnesota[12]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data ▪ Excludes small businesses (as defined by the Small Business Administration)	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive

State	Applicability	Personal Data	Sensitive Data
Montana[13]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
Nebraska[14]	▪ Entities conducting business in the state or producing products or services consumed by residents ▪ Includes a minimum threshold determined by volume of processing or sale of data ▪ Excludes small businesses (as defined by the Small Business Administration)	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
New Hampshire[15]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
New Jersey[16]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive ▪ Financial information ▪ Credentials allowing access to a financial account ▪ Status as transgender or nonbinary

State	Applicability	Personal Data	Sensitive Data
Oklahoma[17]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
Oregon[18]	▪ Entities conducting business in the state or providing products or services to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to a consumer or device that identifies or is linked or reasonably linkable to a household ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive ▪ Status as transgender or nonbinary ▪ Status as victim of a crime ▪ National origin ▪ Genetic or biometric data
Rhode Island[19]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
Tennessee[20]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by annual revenue and volume of processing or sale of data	▪ Information that identifies, relates to, describes, is reasonably capable of being directly or indirectly associated or linked with a consumer ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive

State	Applicability	Personal Data	Sensitive Data
Texas[21]	▪ Entities conducting business in the state or producing products or services consumed by residents ▪ Includes a minimum threshold determined by volume of processing or sale of data ▪ Excludes small businesses (as defined by the Small Business Administration)	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive
Utah[22]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by annual revenue and volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive ▪ Medical history
Virginia[23]	▪ Entities conducting business in the state or producing products or services targeted to residents ▪ Includes a minimum threshold determined by volume of processing or sale of data	▪ Information that is linked or reasonably linkable to an identified or identifiable individual ▪ Does not include de-identified or publicly available data	▪ All data types typically defined as sensitive

Consumer Rights

Privacy laws grant consumers certain rights intended to give them more control over their personal data. Key differences in these consumer rights include the methods by which users give consent for businesses to use their personal data in certain ways; the right to access, port, rectify, and delete this data; and limits on automated decision-making or profiling used for significant decisions, typically those related to lending, employment, housing, and health care.

The vast majority of state privacy laws give consumers the right to opt out of businesses collecting, using, and sharing their personal data, but require businesses to obtain their affirmative, or "opt-in," consent to collect, use, and share their sensitive data, with the exception of California, Iowa, and Utah, whose laws do not contain opt-in provisions for sensitive data. Twelve state privacy laws also include provisions for a universal opt-out mechanism, which allows consumers to opt out of all covered data transfers. Additionally, because of the federal Children's Online Privacy Protection Act, even in states that do not mandate opt-in consent for sensitive data, businesses must obtain "verifiable parental consent" to collect, use, and share personal data from children under age 13.[24]

Every broad state privacy law gives consumers the right to access, port, and delete their personal data, with Iowa and Utah the only states with broad privacy laws that do not give consumers the right to rectify their personal data.

Iowa and Utah also do not place any specific limits on automated decision-making or profiling. The other 19 state privacy laws give consumers the right to opt out of profiling used for significant decisions—such as decisions regarding finances or lending, housing, insurance, education opportunity, criminal justice, employment opportunity, health care services, or access to basic necessities. A 2025 rulemaking in California gives consumers the right to opt out of automated decision-making, including profiling and behavioral targeting, for significant decisions—a broader approach than most states.[25]

Table 3: Consumer rights in state privacy laws

State	Methods of Consent	Right to Access, Port, Rectify, and Delete	Limits on Automated Decision-Making and Profiling
Alabama	▪ Opt-out for most data ▪ Opt-in for sensitive data	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
California	▪ Opt-out ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of automated decision-making for significant decisions
Colorado	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions

State	Methods of Consent	Right to Access, Port, Rectify, and Delete	Limits on Automated Decision-Making and Profiling
Connecticut	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Delaware	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Indiana	▪ Opt-out for most data ▪ Opt-in for sensitive data	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Iowa	▪ Opt-out	▪ Right to access, port, and delete data	▪ None
Kentucky	▪ Opt-out for most data ▪ Opt-in for sensitive data	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Maryland	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Minnesota	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Montana	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Nebraska	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions

State	Methods of Consent	Right to Access, Port, Rectify, and Delete	Limits on Automated Decision-Making and Profiling
New Hampshire	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
New Jersey	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Oklahoma	▪ Opt-out for most data ▪ Opt-in for sensitive data	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Oregon	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Rhode Island	▪ Opt-out for most data ▪ Opt-in for sensitive data	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Tennessee	▪ Opt-out for most data ▪ Opt-in for sensitive data	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Texas	▪ Opt-out for most data ▪ Opt-in for sensitive data ▪ Universal opt-out mechanism	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions
Utah	▪ Opt-out	▪ Right to access, port, and delete data	▪ None
Virginia	▪ Opt-out for most data ▪ Opt-in for sensitive data	▪ Right to access, port, rectify, and delete data	▪ Opt-out of profiling used for significant decisions

Data Holders' Responsibilities

In addition to upholding consumers' privacy rights enumerated in each state law, businesses must also take on certain responsibilities intended to ensure that they protect their consumers' privacy and security. Common responsibilities state privacy laws place on businesses include risk assessments for certain types of data processing, cybersecurity requirements, transparency requirements, data minimization, and purpose specification.

Most broad state privacy laws share similar risk assessment requirements, with the exception of Alabama, Iowa, and Utah, which do not require risk assessments, and California, which clarified its risk assessment requirements in a 2025 rulemaking. Most states require risk assessments before initiating data processing that poses a "heightened risk" to consumers. This typically includes the sale of personal data, processing of sensitive data, processing of personal data for targeted advertising, and processing of personal data for profiling that poses a risk of unlawful or deceptive treatment, unlawful disparate impact, offensive intrusion on private affairs, or financial, physical, reputational, or other substantial injury.

California, meanwhile, requires risk assessments before initiating data processing that poses a "significant risk" to consumers, a much wider scope that includes selling or sharing personal data, using sensitive data, using automated decision-making technology to make a significant decision, using automated processing to infer or extrapolate sensitive traits about a consumer in certain sensitive contexts or based on the consumer's presence in a sensitive location, or developing or training automated decision-making technology or artificial intelligence (AI) using personal data. Businesses must also review risk assessments every three years and update them following any material change to processing activities.[26]

In addition to upholding consumers' privacy rights enumerated in each state law, businesses must also take on certain responsibilities intended to ensure that they protect their consumers' privacy and security.

All 21 broad state privacy laws require businesses to implement "reasonable security practices." Colorado frames this as an explicit "duty of care" to secure personal data and safeguard it from unauthorized acquisition, though the other states' requirements function as implicit duties of care. California additionally requires annual cybersecurity audits for businesses that derive at least 50 percent of their revenue from selling or sharing personal data or earn more than $25 million in annual revenue and conduct large-scale data processing, defined as processing at least 250,000 consumers' data or 50,000 consumers' sensitive data.[27]

In addition, 20 broad state privacy laws require businesses to provide a general privacy notice explaining what types of data they collect and why, the types of data the businesses share with third parties and the types of third parties that receive this data, and how consumers can exercise their privacy rights. California goes a step further by requiring businesses to provide real-time notice at collection and update their privacy policies every 12 months. All 21 laws also require businesses to give explanations of consumers' opt-out rights. California mandates a "Do Not Sell/Share" link that leads to this information, while the remaining states simply require the opt-out disclosure to be "clear and conspicuous."

Table 4: Data holders' responsibilities in state privacy laws

State	Risk Assessments	Cybersecurity Requirements	Transparency Requirements
Alabama	▪ None	▪ Implement reasonable security practices	▪ "Reasonably accurate, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
California	▪ Required before initiating processing that poses a "significant risk" ▪ Reviewed every 3 years ▪ Updated following any material change to processing activities	▪ Implement reasonable security practices ▪ Annual cybersecurity audits for businesses conducting high-risk processing	▪ Notice at collection ▪ Privacy policy updated every 12 months ▪ Opt-out disclosure via "Do Not Sell/Share" link
Colorado	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices ▪ Duty of care	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Connecticut	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Delaware	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Indiana	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure

State	Risk Assessments	Cybersecurity Requirements	Transparency Requirements
Iowa	▪ None	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Kentucky	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Maryland	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Minnesota	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Montana	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Nebraska	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible and clear" privacy notice ▪ "Clear and conspicuous" opt-out disclosure

State	Risk Assessments	Cybersecurity Requirements	Transparency Requirements
New Hampshire	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible and clear" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
New Jersey	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible and clear" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Oklahoma	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible and clear" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Oregon	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Rhode Island	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Accessible and conspicuous" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Tennessee	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure

State	Risk Assessments	Cybersecurity Requirements	Transparency Requirements
Texas	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible and clear" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Utah	▪ None	▪ Implement reasonable security practices	▪ "Reasonably accessible and clear" privacy notice ▪ "Clear and conspicuous" opt-out disclosure
Virginia	▪ Required before initiating processing that poses a "heightened risk"	▪ Implement reasonable security practices	▪ "Reasonably accessible, clear, and meaningful" privacy notice ▪ "Clear and conspicuous" opt-out disclosure

Data minimization requires organizations to collect no more data than is necessary to meet specific needs. The vast majority of broad state privacy laws require businesses to limit their collection of personal data to what is "adequate, relevant, and reasonably necessary." California introduced data minimization via the California Privacy Rights Act, an amendment to its privacy law that requires data collection to be "reasonably necessary and proportionate" to provide or maintain a specific product or service requested by a consumer or meet other requirements, a much more restrictive standard.[28] Maryland also uses this definition, and Connecticut amended its privacy law in 2026 to adopt this definition as well. Only Utah does not explicitly require data minimization.

Purpose specification and limitation, meanwhile, require organizations to disclose to users the purposes for which they are collecting data and not use this collected data for any other reasons. Every state privacy law that includes purpose limitations restricts businesses from processing personal data in a way that is inconsistent with disclosed purposes. Again, only Utah does not explicitly include purpose limitations.

Table 5: Data holders' responsibilities in state privacy laws, continued

State	Data Minimization	Purpose Limitation
Alabama	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
California	▪ Data collection limited to what is "reasonably necessary and proportionate"	▪ Processing must be consistent with disclosed purposes
Colorado	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Connecticut	▪ Data collection limited to what is "reasonably necessary and proportionate"	▪ Processing must be consistent with disclosed purposes
Delaware	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Indiana	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Iowa	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Kentucky	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Maryland	▪ Data collection limited to what is "reasonably necessary and proportionate"	▪ Processing must be consistent with disclosed purposes
Minnesota	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Montana	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Nebraska	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
New Hampshire	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes

State	Data Minimization	Purpose Limitation
New Jersey	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Oklahoma	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Oregon	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Rhode Island	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Tennessee	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Texas	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes
Utah	▪ No explicit data minimization	▪ No explicit purpose limitation
Virginia	▪ Data collection limited to what is "adequate, relevant, and reasonably necessary"	▪ Processing must be consistent with disclosed purposes

Oversight and Enforcement

In order to ensure that businesses comply with their privacy laws, states give enforcement power to their attorneys general. Nine states also give their attorneys general rulemaking authority or the power to create binding regulations that implement, interpret, or define their privacy laws. California's privacy law has also led to the establishment of a separate data protection agency, the California Privacy Protection Agency, which shares enforcement and rulemaking authority with the attorney general.

Penalties vary widely from state to state. The standard penalty of up to $7,500 per violation exists in 13 states. States with higher penalties include Alabama, Colorado, Delaware, Maryland, New Hampshire, New Jersey, and Rhode Island. Connecticut has the lowest maximum penalty of up to $5,000 per violation, whereas Maryland has the highest possible penalty of up to $25,000 per violation for repeat offenders.

California differentiates between "negligent" and "intentional" violations. The former represents a failure to take reasonable steps to prevent harm and carries a lighter fine, while the latter represents deliberate action that results in harm and carries a heftier fine. In California, violations involving children's data also carry higher penalties. Maryland and New Jersey have a

different tiered system, with lighter fines for first infractions and heftier fines for subsequent ones.

California is the only state with a private right of action, which allows users to sue organizations directly for civil penalties. This limited private right of action applies to data breaches of sensitive data arising from businesses failing to maintain reasonable security measures. Plaintiffs can sue for actual damages or statutory damages. Statutory damages are preset amounts defined by the law itself, ranging from $100 to $750 per violation, and are used when actual losses are hard to prove. Actual damages, meanwhile, represent specific, provable financial losses or measurable harm.

Finally, all 21 broad state privacy laws give businesses an opportunity to cure during a defined period when entities can correct or remedy a violation before facing penalties. California's private right of action includes a 30-day cure period to avoid statutory damages but no cure period for actual damages. In 11 states, cure periods for government enforcement are at each state's attorney general's discretion, though of these states, five previously had guaranteed cure periods that were phased out. The remaining 10 states have guaranteed cure periods. These cure periods range from 30 to 90 days: 11 states have 30-day periods and 8 have 60-day periods, with Alabama having a 45-day period and Iowa a 90-day period.

Table 6: Oversight and enforcement mechanisms in state privacy laws

State	Government Enforcement	Private Right of Action	Opportunity to Cure
Alabama	▪ Attorney General has enforcement authority ▪ Up to $15,000 per violation	▪ None	▪ Guaranteed 45-day cure period
California	▪ California Privacy Protection Agency and Attorney General share enforcement and rulemaking authority ▪ Up to $2,500 per negligent violation ▪ Up to $7,500 per intentional violation or violation involving children's data	▪ Limited ▪ Applies to data breaches of sensitive data arising from failure to maintain "reasonable security measures" ▪ Actual damages or statutory damages ▪ $100–750 in damages per consumer per incident	▪ 30-day cure period to avoid statutory damages (does not apply to actual damages) ▪ Discretionary 30-day cure period for government enforcement as of January 1, 2023 ▪ Previously guaranteed
Colorado	▪ Attorney General has enforcement and rulemaking authority ▪ Up to $20,000 per violation	▪ None	▪ Discretionary 60-day cure period as of January 1, 2025 ▪ Previously guaranteed

State	Government Enforcement	Private Right of Action	Opportunity to Cure
Connecticut	▪ Attorney General has enforcement and rulemaking authority ▪ Up to $5,000 per violation	▪ None	▪ Discretionary 60-day cure period as of December 31, 2024 ▪ Previously guaranteed
Delaware	▪ Attorney General has enforcement and limited rulemaking authority ▪ Up to $10,000 per violation	▪ None	▪ Discretionary 60-day cure period
Indiana	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 30-day cure period
Iowa	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 90-day cure period
Kentucky	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 30-day cure period
Maryland	▪ Attorney General has enforcement authority ▪ Up to $10,000 per violation (first violation) ▪ Up to $25,000 per violation (subsequent violations)	▪ None	▪ Discretionary 60-day cure period
Minnesota	▪ Attorney General has enforcement and limited rulemaking authority ▪ Up to $7,500 per violation	▪ None	▪ Discretionary 30-day cure period
Montana	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Discretionary 60-day cure period as of April 1, 2026 ▪ Previously guaranteed

State	Government Enforcement	Private Right of Action	Opportunity to Cure
Nebraska	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 30-day cure period
New Hampshire	▪ Attorney General has enforcement and limited rulemaking authority ▪ Up to $10,000 per violation	▪ None	▪ Discretionary 60-day cure period
New Jersey	▪ Attorney General has enforcement and rulemaking authority ▪ Up to $10,000 per violation (first violation) ▪ Up to $20,000 per violation (subsequent violations)	▪ None	▪ Discretionary 30-day cure period
Oklahoma	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 30-day cure period
Oregon	▪ Attorney General has enforcement and rulemaking authority ▪ Up to $7,500 per violation	▪ None	▪ Discretionary 30-day cure period as of January 1, 2026 ▪ Previously guaranteed
Rhode Island	▪ Attorney General has enforcement authority ▪ Up to $10,000 per violation	▪ None	▪ Discretionary 60-day cure period
Tennessee	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 60-day cure period ▪ Safe harbor
Texas	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 30-day cure period

State	Government Enforcement	Private Right of Action	Opportunity to Cure
Utah	▪ Attorney General has enforcement authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 30-day cure period
Virginia	▪ Attorney General has enforcement and limited rulemaking authority ▪ Up to $7,500 per violation	▪ None	▪ Guaranteed 30-day cure period

TRENDS IN STATE PRIVACY LAWS

The vast majority of broad state privacy laws share many common provisions that could provide Congress with a useful starting point when crafting federal legislation. In fact, there are more significant areas of consensus between state privacy laws than there are significant areas of contention. These include definitions of personal and sensitive data, consumer rights, data holder responsibilities, and enforcement mechanisms.

Compared with the many significant areas of consensus, there are two main areas of contention: the inclusion of a universal opt-out mechanism and whether a law's opportunity to cure is guaranteed or discretionary.

Areas of Consensus Among State Privacy Laws

When it comes to definitions, by far the most common one of personal data or information is "information that is linked or reasonably linkable to an identified or identifiable individual," explicitly excluding anonymous or de-identified data, which enables greater innovation using these forms of data that would not infringe on individual users' privacy. By placing fewer restrictions on anonymous and de-identified data, a federal privacy law would incentivize businesses to rely on these forms of data rather than data that could identify an individual whenever doing so is possible, creating a win-win scenario for businesses and consumers.

The most common categories of sensitive data or information include race or ethnicity, religious beliefs, mental or physical health conditions or diagnoses, sex life or sexual orientation, citizenship or immigration status, uniquely identifying genetic or biometric data, personal data from a known child, and precise geolocation data. If the aim of a privacy law is to protect consumers, then it makes logical sense to impose greater restrictions on categories of personal data that have a greater potential to cause financial, physical, or reputational harm to individuals.

Next, when it comes to consumer rights, by far the most common approach is to give consumers the right to opt out of businesses collecting, using, and sharing their personal data or profiling them for significant decisions and require businesses to obtain consumers' affirmative, or "opt-in," consent to collect, use, and share their sensitive data. This two-tiered consent structure

reduces the significant compliance costs associated with obtaining affirmative consent in most cases while implementing stricter safeguards that protect the most sensitive forms of personal information. Combined with the right for consumers to access, port, rectify, and delete their personal data, which is also present in nearly all state privacy laws, this approach increases transparency around data collection and gives users greater control, especially as it relates to significant decisions such as those related to lending, employment, housing, and health care.[29]

When it comes to responsibilities, nearly all state laws require businesses to conduct risk assessments before processing personal data that poses a "heightened risk" to consumers. Again, this scope targets data processing that has the greatest potential to cause financial, physical, or reputational harm, protecting consumers while minimizing the compliance burden on businesses that do not conduct high-risk data processing, in turn allowing businesses to dedicate fewer resources toward legal compliance and more resources toward innovation.

All state laws require businesses to implement reasonable security practices to protect consumers' personal data. Cybersecurity and data privacy are intrinsically linked: unauthorized access to consumers' personal data puts them at various levels of risk depending on the sensitivity of the data in question. A business that does not implement reasonable security practices cannot effectively safeguard users' privacy. Moreover, by merely requiring reasonable security practices without prescribing specific practices, state privacy laws avoid giving attackers a playbook on what businesses are doing to protect users' privacy and give businesses of all types and sizes increased flexibility to determine what security practices will best protect consumers' personal data depending on the level of risk.

There are more significant areas of consensus between state privacy laws than there are significant areas of contention. These include definitions of personal and sensitive data, consumer rights, data holder responsibilities, and enforcement mechanisms.

Additionally, nearly all state laws require businesses to provide accessible privacy notices and conspicuous opt-out disclosures. These notices and disclosures provide consumers with greater insight into how businesses collect, use, and share their data and inform them on how to exercise their privacy rights. Mandating that these notices and disclosures be accessible and conspicuous is important to ensure that consumers are able to easily find this information. States that avoid overly specific instructions on how businesses should ensure that these notices are accessible and conspicuous allow for greater flexibility and can hopefully avoid scenarios similar to the EU's cookie notification policy, which have led to annoying pop-up cookie banners that the vast majority of users ignore or click through without reading and costs the EU an estimated $2.3 billion each year in compliance costs and decreased productivity from users having to click through these banners.[30]

Nearly all state laws also require businesses to limit data collection to what is "adequate, relevant and reasonably necessary" and limit data processing within "disclosed purposes." These data minimization and purpose specification and limitation policies unfortunately carry high indirect costs by reducing access to data, limiting data sharing, and constraining its use. Data minimization negatively impacts organizations that do not know which data will be most valuable when initially deciding what data to collect, as well as limits organizations' ability to analyze data

in the development of new products and services. Meanwhile, purpose specification and limitation create a barrier to innovation, as organizations cannot reuse collected data for new purposes or apply data analytics to collected data.[31] States with stricter data minimization or purpose specification and limitation policies will impose even higher indirect costs than those with narrower policies will.

In terms of enforcement, all state laws give state attorneys general enforcement powers, and almost no state laws include a private right of action of any kind. The economic cost of privacy enforcement would be much higher if legislation allowed for duplicative or frivolous enforcement via a private right of action that enables users to sue a company directly for violations. This would open the floodgates for unnecessary, baseless lawsuits against organizations that handle personal data, which would disincentivize organizations from offering innovative new products or services that may open them up to liability.

All state laws also include some form of an opportunity to cure. These provisions encourage compliance among good actors—companies that make mistakes but ultimately want to comply with the law. These companies have an opportunity to fix their mistakes without penalty. Meanwhile, regulators can focus on taking action against bad actors that willfully ignore the law.[32]

State privacy laws provide a valuable foundation for federal policymaking, offering practical insight into what works and what does not in protecting consumers and regulating data use.

Areas of Contention

The first major area of contention between different state privacy frameworks is the inclusion of a universal opt-out mechanism. Such a mechanism significantly undermines the compromise between opt-in and opt-out requirements for different types of data. This type of universal opt-out encourages consumers to broadly restrict data sharing rather than use the more granular controls available to them by different data holders, without consideration for the societal implications of less data sharing. Most notably, a universal opt-out would shrink ad revenue for online services—news, apps, games, and more—that consumers get for free today. To make up for the loss in revenue, these services would then need to show more ads (but less-relevant ones) or charge users fees for formerly free apps.[33] Others might simply shut down.

The second major area of contention is whether each law requires its state attorney general to provide an opportunity to cure or leaves that decision to their discretion. A guaranteed opportunity to cure creates a much stronger incentive for compliance among good actors. In the case of a discretionary opportunity to cure, even if businesses quickly address an alleged violation, regulators can still fine them. This forces companies to predict exactly what regulators want, giving them no margin of error in interpreting regulatory guidance as they roll out new products or services because they will otherwise face expensive consequences. It also fails to separate good actors from bad ones, and punishes all companies the same, regardless of their intent or the harm they cause.[34]

RECOMMENDATIONS FOR CONGRESS

State privacy laws provide a valuable foundation for federal policymaking, offering practical insight into what works and what does not in protecting consumers and regulating data use. By comparing these approaches, Congress can identify best practices, avoid unintended consequences, and craft a national privacy framework that is both effective and workable.

Drawing from these lessons, federal data privacy legislation should:

- exclude anonymous and de-identified data from its definition of personal data in order to enable greater innovation using nonsensitive forms of data;
- limit its definition of sensitive data to categories of personal data that have the greatest potential to cause financial, physical, or reputational harm to individuals, protecting individuals from real privacy harms;
- balance the interests of protecting consumers, giving consumers greater control, and enabling innovation through data by giving consumers the right to opt out of businesses collecting, using, and sharing their personal data or profiling them for significant decisions, but require businesses to obtain consumers' affirmative, or "opt-in," consent to collect, use, and share their sensitive data;
- require businesses to conduct risk assessments only before processing personal data that poses a "heightened risk" to consumers, which would minimize the compliance burden on businesses while still protecting consumers from real privacy harms;
- require businesses to implement reasonable security practices to protect consumers' personal data but avoid prescribing specific cybersecurity practices, giving businesses the flexibility they need to adapt to different levels of cyber risks and attackers' ever-evolving methods;
- require businesses to provide accessible privacy notices and conspicuous opt-out disclosures but avoid giving specific instructions on how businesses should ensure that these notices and disclosures are accessible and conspicuous, providing greater transparency to consumers without inconveniencing businesses or consumers;
- avoid including data minimization or purpose specification and limitation requirements so as not to place limits on innovation and flexibility that ultimately benefits consumers;
- avoid creating a private right of action that would unnecessarily expose companies to substantial legal costs and force them to focus more on fighting meritless lawsuits and less on designing safe and innovative products and services for consumers;
- avoid including a universal opt-out mechanism, which would lead to a significant loss in revenue for ad-supported businesses that they would likely pass on to consumers; and
- include a guaranteed opportunity to cure in order to incentivize businesses to comply in good faith and correct mistakes while still leaving room for regulators to punish bad actors that willfully ignore the law.

CONCLUSION

The state privacy patchwork in the United States is expensive for businesses and confusing for consumers. Congress should act quickly to pass a federal privacy law that establishes a uniform national standard by preempting all state privacy laws.

However, Congress can learn from state privacy laws in order to do so. In the areas of consensus between state privacy laws, Congress can see where lawmakers at the state level have reached workable compromises between different interests. In the areas of contention between state privacy laws, Congress can compare provisions that are more restrictive against provisions that are more narrowly targeted and evaluate the impact each of those provisions would have on businesses and consumers at the national level.

The end result should be a targeted federal data privacy law that enshrines important consumer privacy rights, prevents real privacy harms, preempts inconsistent state laws, and minimizes the impact on productivity and innovation. This approach would strike a balance that benefits consumers and businesses and allows the data-driven Internet economy to continue to thrive.

About the Author

Ash Johnson is a senior policy manager at ITIF, specializing in Internet policy issues including privacy, security, platform regulation, e-government, and accessibility for people with disabilities. Her insights appear in numerous prominent media outlets such as *TIME*, the *Washington Post*, *NPR*, *BBC*, and *Bloomberg*. Previously, Ash worked at Software.org: the BSA Foundation, focusing on diversity in the tech industry and STEM education. She holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. Fla. Stat. § 501.702.
2. Cal. Civ. Code § 1798.140.
3. Alabama HB 351 enrolled.
4. Cal. Civ. Code § 1798.100 et seq.
5. CO Rev Stat § 6-1-1301 et seq.
6. Conn. Gen. Stat. § 42-515 et seq.

7. 6 Del. C. § 12D-101 et seq.
8. IN Code § 24-15.
9. Iowa Code § 715D.
10. KRS §§ 367.3611 to 367.3629.
11. MD Commercial Law Code §§ 14-4701 to 14-4713.
12. MN Stat §§ 325M.10 to 325M.21.
13. MT Code § 30-14-2801 et seq.
14. NE Code §§ 87-1101 to 87-1130.
15. NH Rev Stat § 507-H.
16. NJ Rev Stat § 56:8-166.4 et seq.
17. O.S. 75A §§ 300 to 315.
18. ORS 646A.570 to 646A.589.
19. RI Gen L § 6-48.1.
20. TN Code §§ 47-18-3301 to 47-18-5706.
21. Tex. Bus. & Com. Code § 541.
22. UT Code § 13-61-101 et seq.
23. Va. Code Ann. §§ 59.1-575 to 59.1-585.
24. 15 U.S.C. § 6502.
25. 11 CCR § 7221.
26. 11 CCR § 7150-7157.
27. 11 CCR § 7120-7124.
28. 11 CCR § 7221.
29. Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules" (ITIF, October 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules.
30. Daniel Castro and Alan McQuinn, "The Economic Costs of the European Union's Cookie Notification Policy" (ITIF, November 2014), https://www2.itif.org/2014-economic-costs-eu-cookie.pdf.
31. Ash Johnson and Daniel Castro, "Maintaining a Light-Touch Approach to Data Protection in the United States" (ITIF, August 2022), https://itif.org/publications/2022/08/08/maintaining-a-light-touch-approach-to-data-protection-in-the-united-states/.
32. Ash Johnson, "Proposition 24 Took Away the Only Good Thing in California's Privacy Legislation" (ITIF, November 4, 2020), https://itif.org/publications/2020/11/04/proposition-24-took-away-only-good-thing-california-privacy-legislation/.
33. Ash Johnson, "Review of the Proposed American Privacy Rights Act" (ITIF, April 12, 2024), https://itif.org/publications/2024/04/12/review-of-proposed-american-privacy-rights-act/.
34. Johnson, "Proposition 24 Took Away."