Connected Commerce Council

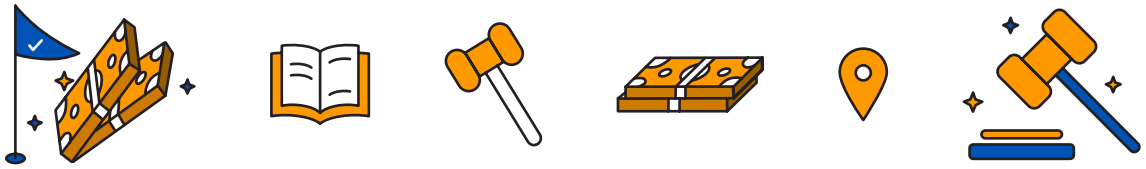
Breaking Through the Privacy Patchwork:

A Growing Burden on Small Businesses

Connected Commerce Council

About 3C

The Connected Commerce Council (3C) is dedicated to empowering small businesses by advocating for policies that enhance innovation, affordability, and accessibility in the digital economy. The organization provides resources, research, and training to help small businesses leverage digital tools, including AI, to grow and compete effectively. Our initiatives focus on addressing key issues such as online advertising, data privacy, and the benefits of technology platforms for small businesses.



The Growing Patchwork of State Laws: Compliance a Nightmare

50 States, 50 Different Laws?
That's impossible for small businesses.

- Over 20 states have or are enacting their own privacy laws, each with different rules, definitions, and enforcement mechanisms.
- The volume of regulations is overwhelming with more than 1,000 pages (and growing).
- These laws apply to any business collecting data from residents in those states, no matter where the business is located.
- Even a small online shop or blog with a contact form may be required to comply with multiple, conflicting laws.

While we are not the intended target for these laws, the prospect of tracking and determining if we have to comply with multiple state data privacy laws, let alone 50, is daunting, if not impossible.

— Clark Twiddy, Twiddy & Co (Duck, NC)

A $50,000 Problem

The Cost of Compliance for Small Businesses

- Privacy compliance is often designed with large corporations in mind, not small businesses.
- Small businesses face thousands in legal and technical costs to comply with multiple state laws.
- Fines for non-compliance can devastate a small business.
- Constantly changing requirements across states add to the time, confusion, and risk

Compliance Costs (Per Year)

$50,000
Average cost /year

≤ $60,000
Additional cost /year

≤ $120,000
Legal fee /year

Fines for Non-Compliance

$7,500
Virginia CDPA /violation

$20,000
Colorado CDPA /violation

≤ $20,000,000
GDPR (EU) /violation

The Solution - A Federal Privacy Law That Works for Small Businesses

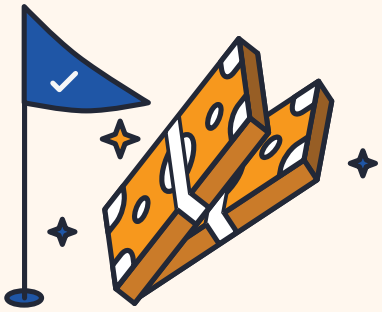
One Law. One Standard. A Fair Playing Field.

Key benefits of a National Privacy Law

Small businesses care about their customers' privacy. But they need clear, consistent rules they can actually follow. A strong national privacy law would eliminate the confusion and high costs of the current state-by-state approach, providing small businesses with the clarity and certainty they need to operate efficiently.

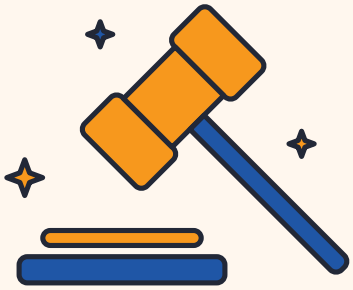
One Rule for All Businesses

No more state-by-state confusion.



Lower Costs

A single compliance process instead of 20+.



Fewer Lawsuits

Less risk of predatory legal action.

Market Growth

Enable small businesses to serve customers in every state.

Momentum for a Federal Solution is Growing

Lawmakers recognize the need for a national privacy law that balances consumer protection with manageable compliance for small businesses.

Senator Ted Cruz (R-Texas), Chair of the Senate Commerce Committee, has pointed to the Texas Data Privacy and Security Act (TDPSA) as a blueprint for federal legislation. Unlike California's more rigid privacy laws, the TDPSA aims to safeguard data while keeping compliance reasonable for small businesses. A federal law following this approach would provide clarity, consistency, and lower compliance costs for small businesses.

With momentum building, small businesses should prepare by adopting best practices aligned with business-friendly state laws like Texas'. A clear, fair federal privacy law is overdue.

It's Time for Action

Congress must act now. Small businesses deserve a clear, fair, and national standard.

Table of Contents

Executive Summary

Small businesses are the backbone of the American economy. Now more than ever, they leverage digital tools to compete in the marketplace. But a growing patchwork of state data privacy laws is making it harder for small businesses to use these tools to grow their business and reach their customers. As of April 2025, 20 states have enacted their own data privacy laws with varying rules and compliance requirements. While protecting consumer privacy is critical, the lack of a uniform framework is creating real-world burdens for small businesses, with many spending more time and money navigating compliance rules and less time focusing on customers, operations, and growth. The message from small businesses is clear: they want to do right by their customers and respect privacy. But they need clear, consistent rules to follow. A national privacy law would provide that clarity, ensuring consumer protections without making it impossible for small businesses to compete.

Caught in the Crossfire: Small Businesses Navigating the Patchwork Problem

Most small businesses don't have their own legal departments or compliance teams. They operate and focus on what they do best: serving their customers. But today, those same businesses are being pulled into a complex legal landscape they're not equipped to handle.

Small businesses have online stores that are accessible and open for all customers nationwide. Imagine a small business owner based in Tennessee, fulfilling an order for a customer residing in California. This seemingly simple transaction suddenly throws the business into a complex web of varying state privacy laws. While the Tennessee business owner might operate under Tennessee's state privacy regulations, they still must comply with the California Consumer Privacy Act (CCPA) requirements due to the customer's location.

These variations add up. Some states define "personal information" differently. Others include a "private right of action," allowing individuals to file lawsuits. For a small business trying to do the right thing, the rules are constantly shifting, and the consequences for getting it wrong can be severe. That's why small businesses need a federal privacy law that would replace this patchwork with a clear, consistent standard. A well-crafted federal law would provide strong protections for consumers, while ensuring small businesses can continue to grow and use the digital tools they depend on, such as online advertising, data-driven marketing, and customer insights. Without a balanced approach, restrictive privacy laws could limit small businesses' ability to reach customers, drive sales, and compete.

This playbook outlines the existing state privacy laws, key considerations for small businesses, and the importance of a federal privacy law.

Why This Matters: The Patchwork of Privacy Laws Stifles Small Business Growth

Small businesses rely on data-powered digital ads to reach customers affordably and effectively. Without access to consumer data, they cannot reach the right customers and grow their business. A growing patchwork of state privacy laws is making it harder and more expensive for small businesses. These laws vary widely, forcing small businesses with customers in multiple states to comply with different, often conflicting regulations.

Some laws, like California's, include a private right of action (PRA), allowing lawsuits against businesses for alleged noncompliance. This opens the door for predatory legal actions that pressure small businesses into costly settlements. Compliance with these laws is also expensive. Information Technology & Innovation Foundation (ITIF) predicts state-by-state regulations could cost small businesses **$50 billion annually in legal fees, conducting privacy audits, and hiring data protection officers**. These costs ultimately get passed on to consumers through higher prices and reduced discounts, disproportionately affecting low-income households.

A federal privacy law that preempts state regulations would provide consistency and reduce legal costs. This would also ease the burden on small business owners, who already juggle multiple responsibilities in their daily operations. The current patchwork of state privacy laws adds another layer of complexity, forcing small businesses to keep up with an ever-changing legal landscape. Instead of navigating confusing and inconsistent regulations, small businesses should be able to allocate their time and resources to focus on growth and serving their customers. Therefore, Congress must act now to establish a clear, nationwide privacy law protecting consumers and small businesses.

Relevant Definitions to Understand Privacy Terms

As small business leaders and policymakers, we must understand that privacy terms can differ significantly from one state to another. This is a glossary of terms for awareness:

CCPA: California Consumer Privacy Act signed into law on June 28, 2018, making it the first state-level privacy law in the US. The CCPA applies to businesses that collect California residents' personal information. (Source: **CPPA**)

Consumer: This refers to residents of a specific state's privacy laws. An individual who purchases or uses goods and services, or whose personal information is collected, used, or shared by businesses. (Source: **California's Office of the Attorney General**)

Controller: The entity (person, company, or organization) determines how to process personal data. Controllers have primary responsibility for data protection compliance. (Source: **European Data Protection Board**)

Data Minimization: The idea that entities should only collect, use, and transfer personal data that is "reasonably necessary and proportionate" to provide or maintain a product or service requested by the individual. This standard better aligns business practices with what individuals expect and puts people back in control of their own data. (Source: **Electronic Privacy Information Center**)

First-party cookies: Small text files created and stored by the website you're visiting directly. These files remember user preferences, login information, and other data to improve your experience on that specific site (Source: **Google Policies**)

Opt-In: An option that allows consumers to choose to have their personal information collected, used, or shared for certain purposes, such as targeted advertising or data sales. (Source: **IAPP**)

Opt-Out: An option that allows consumers to choose not to have their personal information collected, used, or shared for certain purposes, such as targeted advertising or data sales. For example, the language variation includes, "do not sell or share my personal information" or "do not sell my personal information." (Source: **IAPP**)

Personally Identifiable Information (PII): Information that can be used to identify a person, such as their name, address, or biometric data (Source: **United States Department of Labor**)

Personal Data: Any information that is not publicly available and can be used to identify a specific individual. Some examples of personal data may include a home address, a driver's license number or state identification number, passport information, a financial account number, login credentials, and browsing history. (Source: **General Data Protection Regulation**)

Private Right of Action (PRA): A legal tool often found in federal and state laws that grants an individual or private party the authority to file a civil lawsuit against another party or a business for alleged harm (Source: **Chamber of Commerce Institute for Legal Reform**)

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Source: **General Data Protection Regulation**)

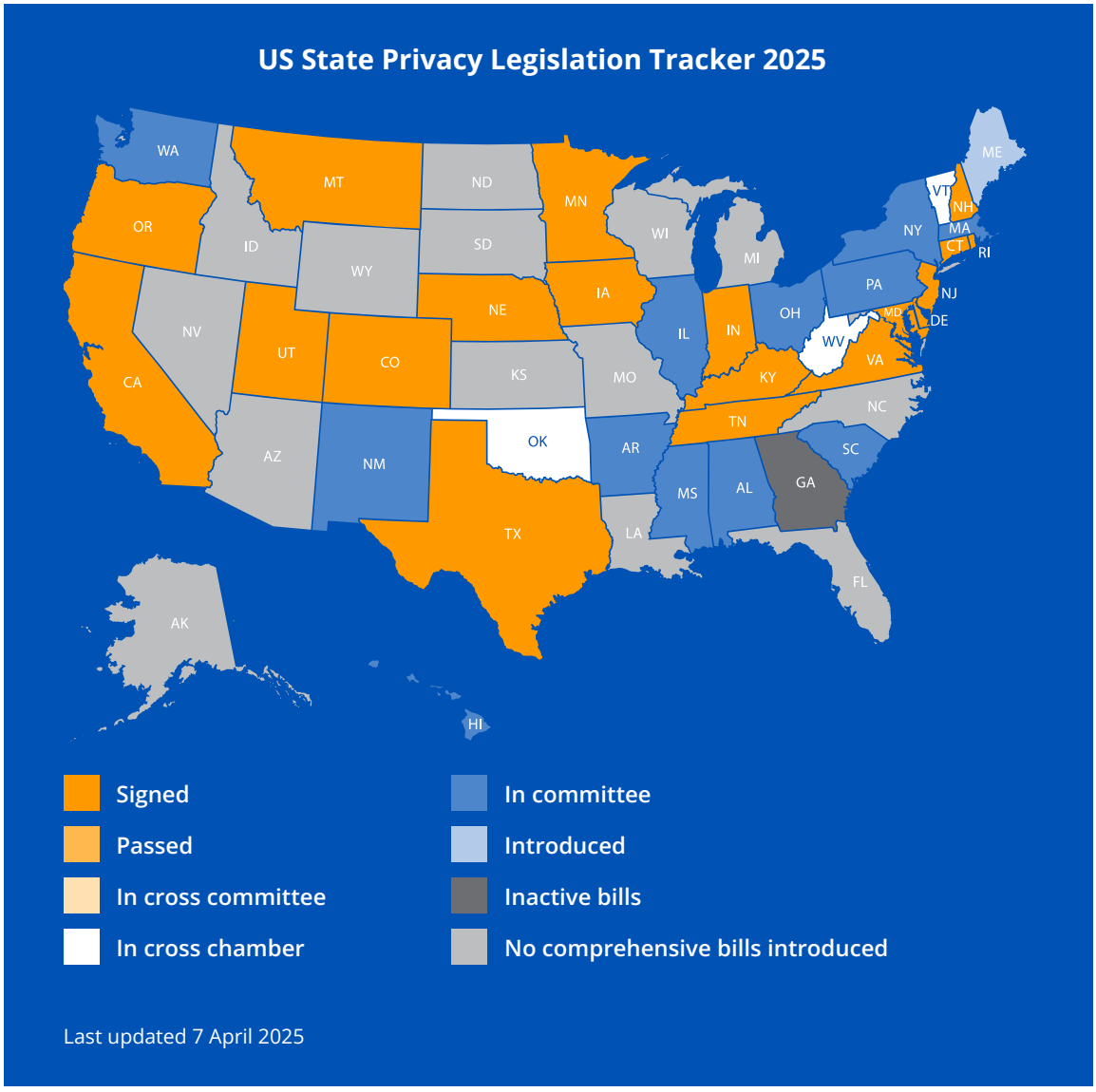
Small business: The Small Business Administration (SBA) defines a U.S. small business as a concern that:

- Is organized for profit
- Has a place of business in the U.S.
- Operates primarily within the U.S. or makes a significant contribution to the U.S. economy through payment of taxes or use of American products, materials, or labor
- Is independently owned and operated and is not dominant in its field on a national basis. (**Code of Federal Regulations**)

Targeted Advertising: A form of online advertising that uses consumer data and behavioral insights to deliver personalized ads to specific audiences based on their interests, demographics, or browsing history. (Source: **New America**)

Third-party cookies: Cookies created by domains other than the one you're currently visiting. They're often used for tracking users across websites, targeted advertising, and analytics. (Source: **Google Developer**)

The Privacy Tug-of-War: Complexity of Opt-In or Opt-Out



As of April 2025, 20 states have signed and enacted privacy laws, but more states are expected to take action on privacy legislation. These requirements have not been uniform across the implementing states and have created a patchwork of laws with widely varying consent standards.

The key area of concern among these state laws is the consent standard for data collection and processing. Some states mandate an opt-in approach, requiring small businesses to obtain explicit consumer consent before collecting or processing personal data. Others adopt an opt-out model, which allows data collection by default unless consumers actively decline. The confusing landscape of opt-in and opt-out requirements creates significant challenges for small businesses, particularly those operating across multiple states. For example, a small business may need to implement opt-in mechanisms for sensitive data in Colorado and Virginia. Still, a business must maintain an opt-out system for general consumer data in California.

Navigating multiple states' compliance frameworks often requires developing separate data processing systems and customizing privacy policies for different states, which means small businesses have no choice but to increase their operational costs and administrative burdens.

The Current 20 States with Effective Privacy Laws

State	Effective Date	Applicability	Cure Provisions & Cure Periods	Private Right of Action	Violation Fee
California Consumer Privacy Act (CCPA)	*January 1, 2023*	■ For-profit entities who: ■ Conducts business in California; Have a gross annual revenue **exceeding $25 million in the preceding year**. ■ Annually buy, sell, or share the personal information of **100,000** or more California residents or households ■ Derive **50% or more of their annual revenue from selling** California residents' personal information.	Opportunity to Care 30-day cure period	*Yes, but limited*	Up to $2,500 for each unintentional violation and $7,500 for each intentional violation
Colorado Privacy Rights Act (CPRA)	*July 1, 2023*	Entities who: ■ Conducts business in Colorado or delivers products or services to Colorado residents; AND ■ Control or process the personal data of **≥ 100,000** Colorado residents during a calendar year, OR ■ **≥ 25,000** Colorado residents and derive revenue or receive a discount on the price of goods or services from the sale of "personal data.	Right to Cure (Until Expiration) 60-day cure period	*No*	$2,000 to $20,000 per violation, with a maximum penalty of $500,000 for a series of violations
The Connecticut Data Privacy Act (CTDPA)	*July 1, 2023*	For-profit entities who: ■ Conducts business in Connecticut or produces products or services targeted to residents of Connecticut; AND ■ During the prior calendar year, control or process the personal data of **≥ 100,000** Connecticut residents, excluding personal data controlled or processed solely to complete a payment transaction ■ **≥ 25,000** Connecticut residents and derive **over 25% of their gross revenue** from the sale of personal data.	Right to Cure (Until Expiration) 60-day cure period	*No*	Up to $5,000 per violation

State	Effective Date	Applicability	Cure Provisions & Cure Periods	Private Right of Action	Violation Fee
Delaware Personal Data Privacy Act (DPDPA)	*January 1, 2025*	Entities who: ■ Conducts business in Delaware or produce products or services targeted to Delaware residents; AND ■ During the prior calendar year, **control or process** the personal data of ≥ 35,000 Delaware residents, excluding "personal data" controlled or processed solely to complete a payment transaction; OR ■ **≥ 10,000** consumers and derive **more than 20% of their gross revenue** from the sale of personal data.	Right to Cure (Until Expiration) 60-day cure period	*No*	Up to $10,000 per violation
Florida Digital Bill of Rights (FLDBOR)	*July 1, 2024*	For-profit entities who: ■ Conducts business within the state of Florida and generates **over $1 billion** in annual global revenue; AND ■ Derives 50% of its global gross revenue from selling online ads; OR ■ Operates an app store offering at least **250,000** different software applications for consumers to download and install; OR ■ Operates a consumer smart speaker and voice command service with an integrated virtual assistant connected to a cloud computing service.	Opportunity to Cure 45-day cure period	*Yes*	Up to $50,000 per violation
Indiana Consumer Data Protection Act (INCDPA	*January 1, 2026*	Entities who: ■ Conduct business in Indiana or produce products or services targeted at Indiana residents; ■ Control or process "personal data" of at least 100,000 Indiana consumers; OR ■ Control or process "personal data" of at least 25,000 Indiana consumers and derive more than 50% of gross revenue from the sale of personal data.	Right to Cure 30-day cure period	*No*	Up to $7,500 per violation

State	Effective Date	Applicability	Cure Provisions & Cure Periods	Private Right of Action	Violation Fee
Iowa Data Privacy Law (IDPL)	*January 1, 2025*	For-profit entities who: ■ Conduct business in Iowa or produce products or services targeted to Iowa residents ■ Control or process personal data of at least **100,000** consumers; or ■ Control or process "personal data" of at least **25,000** consumers and derive **over 50% of gross revenue** from the sale of personal data.	Right to Cure 90-day cure period	*No*	Up to $7,500 per violation
Kentucky Consumer Data Protection Act (KYCDPA)	*January 1, 2026*	Persons who: ■ Conducts business in Kentucky or produces products or services targeted to residents of Kentucky; AND ■ During the calendar year, **control or process** personal data of **≥ 100,000** consumers; OR ■ **≥ 25,000** consumers and derive **over 50% of gross revenue** from the sale of personal data.	Right to Cure 30-day cure period	*No*	Up to $7,500 per violation
Maryland Online Data Privacy (MODPA)	*October 1, 2025*	A person who: ■ Conducts business in Maryland or produces products or services targeted to residents of Maryland; AND ■ During the calendar year, **control or process** personal data of **≥ 35,000** consumers, excluding personal data controlled or processed for the purpose of completing a payment transaction; OR ■ **≥ 10,000** consumers and derived **more than 20% of gross revenue** from the sale of personal data.	Right to Cure 60-day cure period	*No*	Up to $10,000 for each violation and $25,000 per violation for subsequent violations.

State	Effective Date	Applicability	Cure Provisions & Cure Periods	Private Right of Action	Violation Fee
Minnesota Consumer Data Privacy Act (MCDPA)	*July 31, 2025*	Legal entities who: ■ Conducts business in Minnesota or produces products or services targeted to residents of Minnesota; AND ■ During a calendar year, control or process personal data of **100,000** or more consumers, excluding personal data controlled or processed for the purpose of completing a payment transaction; OR ■ Derive **over 25% of gross revenue** from the sale of personal data and process or control personal data of **25,000** consumers or more.	Right to Cure 30-day cure period	*Yes*	Up to $7,500 per violation
Montana Consumer Data Privacy Act (MTCDPA)	*October 1, 2024*	For-profit entities who: ■ Conduct business in Montana or produce products or services targeted to residents of Montana; AND ■ **Control or process** the personal data of **≥ 50,000** Montana residents, excluding "personal data" controlled or processed only for the purpose of completing a payment transaction; OR ■ **≥ 25,000** Montana residents and derive **over 25% of gross revenue** from the sale of personal data.	Right to Cure 60-day cure period	*No*	Does not specify a civil penalty amount
Nebraska Data Privacy Act (NEDPA)	*January 1, 2025*	Entities who: ■ Conduct business in New Hampshire or provide services that target New Hampshire residents. ■ During a one-year period, control or process **≥ 35,000** unique consumers, excluding personal data controlled or processed solely for the purpose of payment transactions; OR ■ **≥ 10,000** unique consumers and derive **more than 25% of gross revenue** from the sale of personal data.	Right to Cure 30-day cure period	*No*	$7,500

State	Effective Date	Applicability	Cure Provisions & Cure Periods	Private Right of Action	Violation Fee
New Hampshire Data Privacy Act (NHDPA)	January 1, 2025	Entities who: ▪ Conduct business in New Hampshire or provide services that target New Hampshire residents. ▪ During a one-year period, **control or process ≥ 35,000** unique consumers, excluding personal data controlled or processed solely for the purpose of payment transactions; OR ▪ **≥ 10,000** unique consumers and derive **more than 25% of gross revenue** from the sale of personal data.	Right to Cure 60-day cure period	*No*	$10,000
New Jersey Data Privacy Law (NJDPL)	*January 15, 2025*	Entities who: ▪ Conduct business in New Jersey or produce products or services that are targeted to New Jersey residents, AND ▪ During the calendar year, **control or process** the personal data of **≥ 100,000** New Jersey residents, excluding data controlled or processed solely for the purpose of completing a payment transaction; or ▪ **≥ 25,000** New Jersey residents and derive revenue or receive a discount on the price of any good or services from the sale of personal data.	Right to Cure 30-day cure period	*No*	Up to $10,000 for an initial offense and $20,000 for later offenses
Oregon Consumer Privacy Act (OCPA)	*July 1, 2024*	Entities who: ▪ Conduct business in Oregon or provide products or services to Oregon residents ▪ During the calendar year, **control or process** the personal data of **≥ 100,000** Oregon consumers, excluding data controlled or processed solely for the purpose of completing a payment transaction; OR ▪ **≥ 25,000** Oregon consumers and derive **more than 25% of gross revenue** from the sale of personal data.	Right to Cure 30-day cure period	*No*	$7,500

State	Effective Date	Applicability	Cure Provisions & Cure Periods	Private Right of Action	Violation Fee
Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)	January 1, 2026	For-profit entities who: ▪ Conduct business in Rhode Island or produce products or services that are targeted to Rhode Island residents; ▪ During the preceding calendar year, **control or process** the personal data of **≥ 35,000** Rhode Island customers, excluding data controlled or processed solely for the purpose of completing a payment transaction; or ▪ **≥ 10,000** Rhode Island customers and derived **more than 20% of gross revenue** from the sale of personal data.	Not applicable	*No*	Up to $10,000 per violation, in addition to the up to $500 per intentional disclosure of personal data
Tennessee Information Protection Act (TIPA)	*July 1, 2025*	For-profit entities who: ▪ Have annual revenue exceeding **$25 million**; AND ▪ **Control or process** personal information of **≥ 175,000** Tennessee consumers during a calendar year; OR ▪ **≥ 25,000** Tennessee consumers and derive **more than 50% of gross revenue** from the sale of personal information.	Right to Cure 60-day cure period	*No*	$7,500
Texas Data Privacy and Security Act (TDPSA)	*July 1, 2024*	For-profit entities who: ▪ Conducts business in Texas or produces products or services consumed by Texas residents; ▪ Processes or engages in the sale of personal data; ▪ Does not identify as a small business as defined by the United States Small Business Administration.	Right to Cure 30-day cure period	*No*	$7,500

State	Effective Date	Applicability	Cure Provisions & Cure Periods	Private Right of Action	Violation Fee
Utah Consumer Privacy Act (UCPA)	December 31, 2023	For-profit entities who: ■ Conduct business in Utah or produce a product or service targeted to Utah residents ■ Have an annual revenue exceeding **$25 million**; AND ■ **Control or process** personal data of **≥ 100,000** Utah residents during a calendar year; OR ■ **≥ 25,000** Utah residents and derive **over 50% of their gross revenue** from the sale of personal data.	Right to Cure 30-day cure period	*No*	$7,500
Virginia Consumer Data Protection Act (VCDPA)	January 1, 2023	For-profit entities who: ■ Conduct business in Virginia or produce products or services targeted to Virginia residents ■ **Control or process** the personal data of **≥ 100,000** Virginia residents during a calendar year; OR ■ **≥ 25,000** Virginia residents and derive **more than 50% of gross revenue** from the sale of personal data.	Right to Cure 30-day cure period	*No*	$7,500

Privacy Law Insights From Small Business Leaders

These quotes come directly from small business leaders who share their experiences regarding the real-world effects of data privacy regulations on their businesses.

Small Businesses Balance Consumer Privacy with Customer Engagement

"As small business owners and advisors, we can say unequivocally that folks like us care deeply about customers' privacy. Running a small business is tough – and small business owners are passionate about succeeding by offering terrific products and services. That means they need to be able to get to know and communicate with their customers. That's good business – and it shouldn't be illegal."

– **Bryan Toston**, Kraken Creative & Jason Stock, Firecracker Software

Bryan Toston is the founder and lead designer of small business advisory Kraken Creative. Jason Stock is the founder of Firecracker Software.

Source: The Spokesman-Review: **Bryan Toston and Jason Stock: The American Privacy Rights Act holds promise – and significant perils – for small businesses**

Data-Powered Advertising is Essential for Small Business Growth

"Lawmakers also need to understand that data-powered advertising and marketing is critical to small, specialty businesses like ours. We can't afford to run TV ads or waste money sending digital ads to people who aren't interested in our products. Data-powered digital ads let us make the most sales with the fewest ad dollars, which keeps our prices low and our business growing. They also help our customers find the foods they've been longing for."

– **Adebukolah Ajao**, Destiny African Market

Adebukola Ajao serves as marketing director at Destiny African Market in Randolph. Her mother, Sola Ajao, founded the business in 1986.

Source: Boston Business Journal: **Commentary: New data privacy regs could hurt my mom's African foods shop**

Restrictive Data Privacy Laws Limit the Reach of the Right Audience

"Proposed data limits mean we'll no longer be able to benefit from our ad partners' data processing. That will make it almost impossible to send the right ads to the right audience, which means we'll have to spend more money on more ads that are less effective — a terrible blow to our bottom line."

– **Adebukolah Ajao**, Destiny African Market

Adebukola Ajao serves as marketing director at Destiny African Market in Randolph. Her mother, Sola Ajao, founded the business in 1986.

Source: Boston Business Journal: **Commentary: New data privacy regs could hurt my mom's African foods shop**

The Burden of Compliance Costs Could be Transferred to Consumers

"Lawmakers need to understand that data-powered digital ads really make a huge difference. Without them, more than two-thirds of Minnesota small businesses would have to raise prices to make up for falling sales."

– **Jeff Taxdahl**, Thread Logic

Jeff Taxdahl is the owner of Thread Logic, a custom-embroidery business, in Jordan, Minnesota.

Source: Duluth News Tribune: **Statewide View: Proposed data-privacy law would harm Minnesota businesses like mine**

Data-Powered Digital Ads Allow Small Businesses to Maximize ROI

"Unlike big companies, we can't afford to run national ad campaigns or send digital ads to everyone shopping for makeup. Instead, we rely on our digital ad partners to help us cheaply and effectively reach people likely to be interested in our specialty products. Our partners do that with light-speed data analysis, not "surveillance." Data-powered digital analysis also lets us see which ads work best, so we can make the most sales with the fewest ads. That saves us time and money we can use to improve our offerings and grow our business. It also lets us keep our products affordable and honor our promise to give part of our profits to organizations supporting Indigenous peoples."

– **Cece Meadows**, Prados Beauty

Cece Meadows founded Prados Beauty, an Indigenous-owned cosmetic and beauty tool store located in Las Cruces, New Mexico– the traditional homelands of the Piro-Manzo-Tiwa people.

Source: Las Cruces Sun News: **Proposed data privacy law would devastate small businesses serving minorities** (Cece Meadows, Prados Beauty)

The Patchwork of Data Privacy Laws Hurts Small Businesses

"Small businesses need national digital privacy legislation to replace today's tangle of state privacy laws. But that legislation shouldn't prevent us from finding and selling to customers. Data-powered digital marketing and advertising is incredibly empowering for niche- and minority-oriented businesses and the customers we serve. I urge Congress to strive for balanced legislation that will help–not hurt–small businesses like mine."

– **Cece Meadows**, Prados Beauty

Cece Meadows founded Prados Beauty, an Indigenous-owned cosmetic and beauty tool store located in Las Cruces, New Mexico– the traditional homelands of the Piro-Manzo-Tiwa people.

Source: Las Cruces Sun News: **Proposed data privacy law would devastate small businesses serving minorities** (Cece Meadows, Prados Beauty)

Small Businesses Call for a National Data-Privacy Law

"It's crucial that [lawmakers] strike the right balance between protecting data privacy and supporting small businesses. We certainly need a national data-privacy law to replace the current patchwork of state laws, which can be as confusing as needing a different driver's license as you travel from state to state."

– **Clark Twiddy**, Twiddy & Company

Clark Twiddy is the president of Twiddy & Company along the Outer Banks of North Carolina, celebrating 45 years as a family-owned business.

Source: The Carolina Journal: **Protecting privacy without undermining small business success**

Small Businesses Leverage Consumer Data to Enhance Customer Experience

"For small businesses like ours, this is not about exploiting data; it's about using it to enhance the customer experience, anticipate needs, and provide outstanding service."

– **Clark Twiddy**, Twiddy & Company

Clark Twiddy is the president of Twiddy & Company along the Outer Banks of North Carolina, celebrating 45 years as a family-owned business.

Source: The Carolina Journal: **Protecting privacy without undermining small business success**

The Bottom Line: Call for a Federal Data Privacy Law

Congress must act now to pass a national data privacy law before more states introduce conflicting regulations. While lawmakers aim to protect consumers, they often overlook the burden these laws place on small businesses that are the backbone of the American economy. This patchwork of privacy creates legal uncertainty, administrative burdens, and potential financial risks for small businesses operating across multiple states. The lack of a federal privacy law exacerbates this issue, requiring small business leaders to juggle varying rules rather than focusing on their growth and community impact. The longer Congress delays action, the more complicated and costly compliance will become, leaving small businesses struggling to keep up. Therefore, we call on Congress to work on a nationwide standard for data privacy that protects consumers, while allowing small businesses to thrive in a digital marketplace.

Connected Commerce
Council