BUCKEYE POLICY BRIEF

A Federalism Opportunity in a Congressional Failure

How States Can Fix the Data Privacy Patchwork

By Logan Kolas
August 10, 2023

Introduction

Concerned with the collection, use, and sale of personal data and information, more than 80 percent of Democrats and Republicans believe Congress should prioritize federal legislation to protect online data.[1] But after more than two decades of Beltway debate, Congress has failed to act, leaving states to fill the legislative void.[2] Two states, California and Virginia, considered comprehensive state privacy legislation in 2018.[3] Today, 12 states have passed comprehensive data privacy laws—with five of them taking effect by the end of 2023.[4] State laws will continue to proliferate and establish well-intended data privacy regimes, but not without a significant cost to businesses and the public.

As more states bring their own unique regulatory frameworks online, the regulated businesses will face an increasingly complex and expensive web of bureaucratic requirements that will further concentrate the market, increase market uncertainty, and raise compliance and operating costs on businesses.[5] Smaller businesses will suffer disproportionally and ultimately consumers will pay higher prices for online user-friendly services that they already take for granted. To alleviate these concerns, states can take several strategic steps. States should collaborate and work together to reduce the number of competing data privacy frameworks across the country. Those frameworks should include compliance incentives such as an affirmative

[1] Sam Sabin, **States are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data**, Morning Consult, April 27, 21

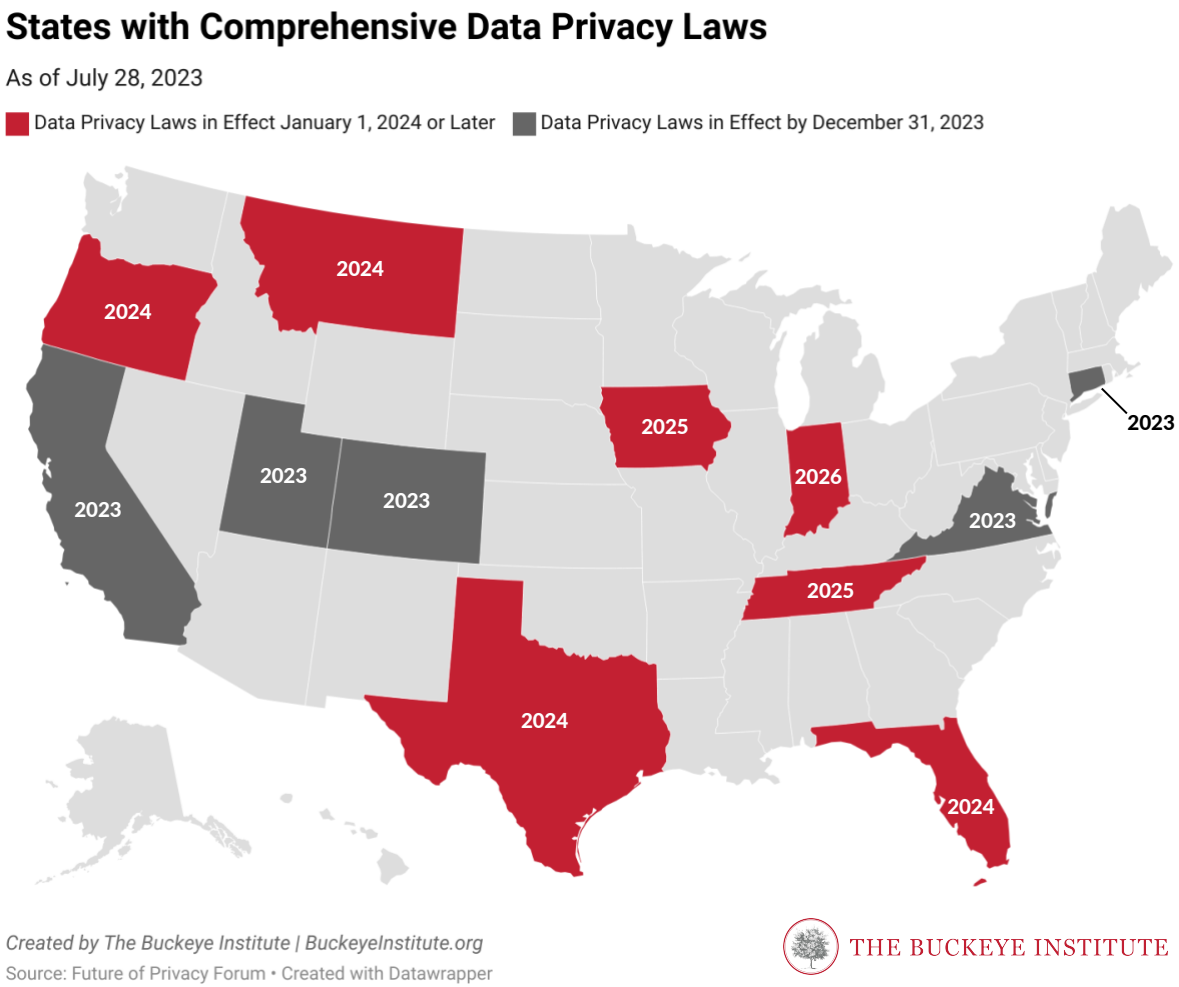
[2] Jessica Rich, **After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law**, The Brookings Institution, January 14, 2021.

[3] Jennifer Huddleston and Gent Salihu, **The Patchwork Strikes Back: State Data Privacy Laws after the 2022-2023 Legislative Session**, Cato at Liberty blog, July 6, 2023.

[4] Keir Lamont and Melis Ulusel, **Effective Dates of New State Privacy Laws**, Future of Privacy Forum, June 30, 2023.

[5] Jason Campbell, Avi Goldfarb, and Catherine Tucker, "**Privacy Regulation and Market Structure**," *Journal of Economics and Management Strategy*, Volume 24, Issue 1 (February 2015): p. 47-73; Berkeley Economic Advising and Research, **Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations**, State of California Department of Justice, Office of the Attorney General, August 2019; Daniel Castro, Luke Dascoli, and Gillian Diebold, ***The Looming Cost of a Patchwork of State Privacy Laws***, Information Technology and Innovation Foundation, January 24, 2022.

defense for adopting industry best-practices standards. States should pursue formal multi-state compacts that will make it easier for businesses to remain compliant across multiple states and jurisdictions. And, in the absence of formal compacts, states should hew closely to a dominant data privacy model and avoid the temptation to craft unique, state-specific regulatory requirements that demand special compliance protocols. Taking these steps will harmonize rules to protect privacy, ease and enhance compliance, and minimize disruptions to preferred online experiences.



The High Cost of a Data Privacy Legal Patchwork

Federal and state data privacy laws impose significant costs on businesses and consumers. Those costs grow as other jurisdictions add their own requirements. Unfortunately, the true cost of overlayed, multi-jurisdiction regulations is often underestimated. The California attorney general's office, for example, projected that California's data privacy law would cost $55 billion—roughly 1.8 percent of the gross state product—but did not factor in similar compliance costs

imposed by other states.[6] Accounting for exported economic burdens, the Information Technology & Innovation Foundation (ITIF) estimated a $46 billion cost to Californians and an additional $32 billion on American businesses and consumers outside California.[7] ITIF estimates that if all states passed their own data privacy laws, such a regulatory patchwork could cost $98 billion to $112 billion annually in out-of-state costs alone. Supporters of comprehensive privacy legislation argue those costs will be frontloaded as compliance become easier over time, but that optimistic, unlikely scenario underestimates the cost of complying with new features and ignores the burden imposed by laws beyond the original jurisdiction. Europe's experience sounds a cautionary note. A Data Grail report found that seven in 10 organization systems will not scale to stay in compliance with Europe's data privacy law as new regulations emerge.[8] Without a future-oriented federal standard that preempts state laws, the United States could suffer a similar fate.

States Must Find Cooperative Solutions

Despite broad agreement by federal lawmakers that the United States needs a federal data privacy law, efforts to pass comprehensive data privacy legislation at the federal level have been squandered. Disagreement largely turns on whether to include a private right of action and a state-law preemption provision.[9] Current signals in Congress suggest federal data privacy legislation will be a rehash of the American Data Privacy and Protection Act that failed to pass after a majority of the California delegation opposed federally preempting California's law.[10] That may change with congressional turnover,[11] but no comprehensive data privacy legislation has been introduced in Congress this term. A federal solution reasserting congressional leadership and mitigating the costs and burdens of a competing patchwork of state laws would be optimal, but only if that federal solution is clear, concise, and limits the bureaucratic power of the unelected agencies that will enforce it. If such a solution remains elusive and untenable, then states should spearhead efforts to harmonize state-level data privacy rules instead. As part of that effort, state policymakers must realize that state privacy laws impact consumers in other states and visa-versa. Accordingly, lawmakers should model legislative proposals on existing laws and resist the temptation to narrowly tailor rules to meet localized constituent demands.

Some state laws already share some general practices such as similar scope provisions, attorney general enforcement power, and general data impact assessments, but parochial variations remain all too common. The Ohio Personal Privacy Act, proposed during the Ohio General Assembly's last term, for example, hewed relatively closely to Virginia's framework but still deviated with respect to affirmative defenses, permanent cure periods, and innovative data

---

[6] **California Estimates $55 Billion Initial Cost for State Businesses to Comply with New Data Privacy Law**, The Association of National Advertisers press release, September 26, 2019.
[7] Daniel Castro, Luke Dascoli, and Gillian Diebold, ***The Looming Cost of a Patchwork of State Privacy Laws***, Information Technology and Innovation Foundation, January 24, 2022.
[8] ***The Age of Privacy: The Cost of Continuous Compliance***, DataGrail, May 2019.
[9] Christiano Lima, **Congress is Reviving the Data Privacy Debate. Don't Hold Your Breath for a Law**, *The Washington Post*, September 24, 2021.
[10] Joseph Duball, **US House Lawmakers Keep Federal Privacy Legislation Top of Mind**, International Association of Privacy Professionals, March 1, 2023.
[11] *Ibid.*

minimization provisions not included in other state legislation. Despite Ohio's commendable improvements, implementing different compliance requirements across multiple states would increase costs for providers and consumers, disrupt the user experience, and divert resources from market-based solutions.[12]

Short of a federal standard, states pursuing comprehensive data privacy legislation should include an affirmative defense for businesses that comply with the National Institute of Standards and Technology (NIST) industry best-practices;[13] pursue data privacy agreements for other states to voluntarily join; and adopt the definitions and statutory language already enacted by other states as closely as possible.

Establish Incentives to Comply with Industry Standards

Ohio lawmakers introduced the Ohio Personal Privacy Act (OPPA) during the General Assembly's last term to give individuals more control over the collection, sale, use, and accuracy of their data. The bill was narrowly tailored with minimum-revenue and minimum revenue triggers, wisely included cure periods for businesses acting in good faith, and avoided foreseeable unintended consequences by not requiring businesses to collect more data than needed in an "ordinary course of business."[14] The bill's best provision—one that should be emulated nationwide—granted companies an affirmative defense if they complied with the NIST data privacy standards. Unfortunately, the useful policies in the proposed OPPA were never enacted, allowing Tennessee to enact the first data privacy legislation with an affirmative defense for NIST compliance.[15]

Critics dismiss a best-practices affirmative defense provision as a giveaway to regulated businesses, but its inclusion actually promotes privacy protection in two ways. First, an affirmative defense incentivizes businesses to comply with an evolving data privacy framework. As technology and data privacy concerns evolve, related legislation could become quickly obsolete, ineffective, and inefficient. But NIST standards are routinely updated, allowing them to evolve and adapt more fluidly than state or federal law. Offering regulated businesses the incentive of an affirmative defense for tracking uniform NIST standards makes industry compliance more attractive, not less. Second, including an affirmative defense for NIST standards compliance in all data privacy laws would lower compliance costs by streamlining privacy compliance across state lines. Importantly, states can pursue this provision alongside other reforms to reduce the legal patchwork while still giving states discretion to adopt privacy regimes tailored to their needs.

Pursue Data Privacy Agreements and Multi-State Compacts

Absent federal comprehensive and preemptive data privacy legislation, states will continue to enact distinct data privacy laws with expensive compliance and enforcement regimes. A better

[12] Jennifer Huddleston, **Data Privacy Day 2023: Where Data Privacy Stands at the Start of 2023**, Cato at Liberty blog, January 27, 2023.
[13] Kaitlin R. Boeckl and Naomi B. Lefkovitz, **NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0**, National Institute of Standards and Technology, January 16, 2020.
[14] Logan Kolas, **Ohio's Data Privacy Tradeoff**, The Buckeye Institute, February 2, 2022.
[15] **House Bill 1181**, Tennessee General Assembly (Last visited May 2, 2023).

approach would be for states to create—and convince other states to join—multi-state, voluntary compacts to enforce identical state data privacy laws. Such interstate compacts have homogenized rules in healthcare, agriculture, professional licensure, taxation, resource conservation, mining, and transportation. They have yet to be used for data privacy.[16] That should change.

The U.S. Constitution's "compact clause" requires congressional approval for states to enter compacts among themselves,[17] but the Supreme Court has taken a "functional interpretation" of the clause to require congressional action only for compacts that increase state power while undermining federal sovereignty.[18] The compacts proposed would not increase state power or undermine federal sovereignty or authority. Congress has debated federal data privacy laws for decades without enacting one, so multi-state agreements to enforce data privacy laws at the state level are unlikely to preempt federal or congressional power. Legal challenges could arise, however, and those prospective costs must be weighed against the likely benefits derived from coordinated state action. Until Congress passes a federal data privacy regime, federal lawmakers at least should make clear that states may "opt-in" to data privacy compacts that fit their policy preferences.

Data privacy compacts would streamline rules and reduce the number of data privacy compliance frameworks for regulated businesses to navigate. States could sort themselves into preferred compact partnerships, with those preferring the NIST standard approach, for example, joining an Ohio-Tennessee compact, while others opt-in to a California-led agreement. Privacy advocates could make their cases for preferred data privacy regimes and encourage state lawmakers to join the compact best-suited to address concerns. Bargaining until compromise is reached, all compact states would streamline rules and reduce regulatory burdens. States unable to agree or reach a compromise would be free to leave or join other compacts instead. Finally, competing compacts could signal to Washington how most state legislatures view data privacy regulation and which components are the most attractive. If many states joined a compact with no private right of action, for example, then Congress may exclude that provision in federal legislation.

Pick a Data Privacy Model and Follow It

With no federal data privacy standard, states have adopted their own data privacy regimes by borrowing legislative language from one another. Using existing statutory language is better than creating new requirements or standards out of whole cloth, but even state efforts to mimic other states must be more carefully executed or risk compounding compliance costs. Most data privacy laws, for example, borrow the scope provisions from California's Consumer Privacy Act or Virginia's Consumer Data Privacy Act. Those statutes limit the law's applicability to businesses that process data of 100,000 consumers and derive 50 percent of gross revenue from data sales.[19]

[16] **Occupational Licensure Compacts**, National Center for Interstate Compacts (Last visited July 28, 2023); **Chart of Interstate Compacts**, Ballotpedia (Last visited July 28, 2023); **United States—Interstate Compacts**, American Law Sources On-line (Last visited July 28, 2023); and **What Are Nursing Compacts**, Nursing CE Central (Last visited July 28, 2023).

[17] Article 1, Section 10, Clause 3, U.S. Constitution.

[18] Stephen P. Mulligan, **Interstate Compacts: An Overview**, Congressional Research Service, August 15, 2022.

[19] **Applicability Thresholds**, Husch Blackwell LLP (Last visited May 2, 2023).

Montana lowered its applicability threshold to 50,000 consumers—significantly expanding the scope of the law—and went further than California in giving consumers a right to revoke consent "data processing," which turns raw data into usable information.[20] Although tailored to Montana's smaller population, lowering the applicability threshold increases compliance costs by creating a unique compliance framework. California may have the strictest comprehensive privacy framework,[21] but companies must now also comply with Montana's unique approach.

Even as states follow other general models, small statutory differences can cause confusion and require expensive legal assistance to ensure compliance, so limiting those differences matters. Tennessee, for example, borrowed most of Virginia's definitions of applicability, but was inspired by Ohio's recently proposed—but unenacted—structure and enforcement provisions.[22] Those provisions may be improvements, but they also make Tennessee a compliance outlier. Ohio's own legislative process that included multiple definition changes, data minimization requirements, and other compromises, would have further distanced Ohio's legislation from Virginia's standard.[23] States must take care to avoid creating unique, conflicting standards and data privacy frameworks that will raise compliance costs. The broad adoption of the Uniform Commercial Code (UCC)—the "backbone of American commerce"—offers guiding precedent. States successfully adopted the UCC to bolster industry confidence in commercial law and its uniform application across legal jurisdictions.[24] No state compacts required. Similarly, states should pick a data privacy model and stick to it, prioritize only the most necessary legal changes, and resist the temptation to diverge from the dominant model.

Conclusion

Congress has abdicated leadership on data privacy, leaving states to craft their own legal frameworks. The result has been a confusing, conflicting legal patchwork of expensive regulatory requirements that disproportionately burden small business, increase market concentration, and ultimately raise consumer prices—all while disrupting the online experience.[25] As Congress dithers, states can mitigate the damage by passing legislation with an affirmative defense for industry standard compliance, pursuing data privacy compacts among themselves, avoiding unique compliance regimes, and hewing more closely to a dominant data privacy framework. States can do what Congress has not, namely pass data privacy legislation that minimizes compliance costs while effectively protecting consumer data privacy.

---

[20] Jennifer Huddleston and Gent Salihu, **The Patchwork Strikes Back: State Privacy Laws after the 2022-2023 Legislative Session**, Cato at Liberty blog, July 6, 2023; Nancy Libin, Michael T. Borgia, John D. Seiver, and Patrick J. Austin, **Montana Consumer Data Privacy Act Signed into Law**, Davis Wright Tremaine LLP, May 23, 2023; and Nikkita Duggal, **What is Data Processing: Cycles, Types, Methods, Steps, and Examples**, SimpliLearn, June 6, 2023.

[21] Tom Spring, **California Adopts Strictest Privacy Law in the US**, ThreatPost, January 2, 2020; and Michael Magotsch and John Isaza, **All Quiet on the Western Front? California Has Stricter Data Protection Laws as of January 1, 2023**, Rimon Law, February 6, 2023.

[22] **House Bill 1181**, Tennessee General Assembly (Last visited May 2, 2023).

[23] **House Bill 376**, The Ohio Legislature (Last visited May 2, 2023).

[24] **Uniform Commercial Code** (Last visited July 20, 2023).

[25] Roslyn Layton, **Protecting Data Privacy Without Destroying the Internet**, Libertarianism.org, October 26, 2018.

About the Author

Logan Kolas is an economic policy analyst with the Economic Research Center at The Buckeye Institute where he researches and writes about the technology and innovation policy, state budget and tax policy, and labor market issues. He is a native of Cincinnati.

THE BUCKEYE INSTITUTE
88 East Broad Street, Suite 1300
Columbus, Ohio 43215
(614) 224-4422
BuckeyeInstitute.org

A Federalism Opportunity in A Congressional Failure: How States Can Fix the Data Privacy Patchwork