# Key Principles for State Data Privacy Laws


By Logan Kolas

THE BUCKEYE INSTITUTE

# Key Principles for State Data Privacy Laws

By Logan Kolas

October 2023

THE BUCKEYE INSTITUTE

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

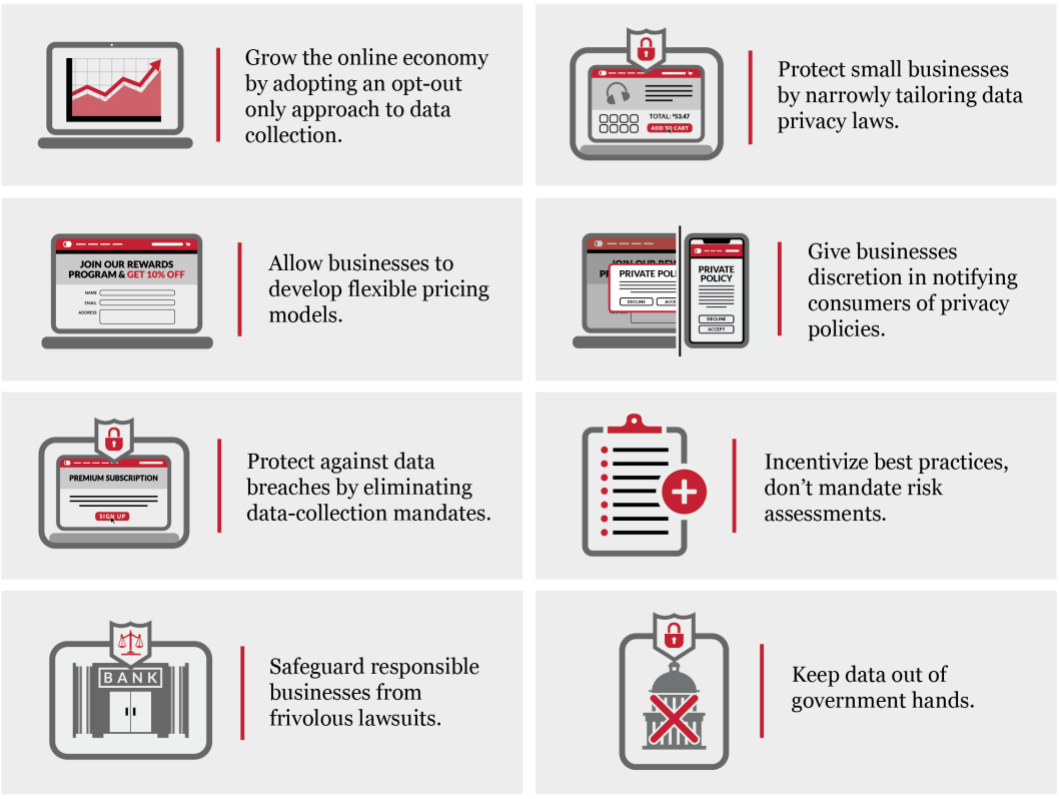
Data privacy battles are waged over the rights and access to information. European countries have historically invested those rights in consumers, while the United States has taken a "sector approach" that prioritizes markets and consumer protection across different economic sectors like healthcare, finance, and education. Both approaches are doomed to fail. By giving consumers the "right" to access, correct, and delete information at-will, Europe has created a type of property right in a resource that cannot be owned and has ignored the fact that different sectors and data types demand different privacy protections. European regimes fail to understand that like a public road, data can be used by many and its use by one does not preclude productive use by others. The U.S. approach, meanwhile, has vested data rights in businesses too heavily and thereby eroded the public's trust. Federal law has kept states from adopting the European privacy approach entirely, but some have still created hybrid data privacy regimes mixing European and American models that have made a mess of competing, conflicting laws. That mix-and-match approach has also failed to balance consumer protections, market needs, and regulatory burdens. Ideally, the United States would abandon the dismal European approach and instead build on technologically free markets, but with over a third of all U.S. states about to have their own data privacy laws by year's end, that best-case scenario seems unlikely.

States can improve upon the European model, however, by adopting eight key principles (Figure 1). Data privacy laws should be narrowly tailored to privacy needs. Executive enforcement should be the province of state attorneys general but narrowly defined so agencies cannot expand the law beyond its original intent. Consumers should be given the option to opt out of sensitive data collection—but they must bear the market consequences of those decisions, so businesses receive the necessary feedback to decide how best to respond to consumer choices with better products and services. That means prices must be nimble enough to fluctuate with changing consumer demands. Similarly, because privacy looks different on different platforms, privacy law should maintain enough flexibility for businesses to notify consumers of their privacy policies. European and new-age American approaches to privacy encouraged businesses to minimize the amount of data they collect—but more time and effort should be spent thinking through alternative methods to minimize the amount of data that new privacy laws themselves encourage businesses to collect. States should avoid requirements that mandate costly risk assessments and instead encourage the adoption of sound internal privacy policies by providing an affirmative defense for compliance with National Institute of Standards and Technology (NIST) best practices. This framework all-encompassing and will encourage dynamic privacy frameworks that

promote collaboration between states and that evolve over time, rather than adherence to privacy laws that quickly become obsolete. Finally, states should closely examine their own legal frameworks to promote practices that better protect consumer data from nefarious actors and data breaches, while also protecting American privacy from warrantless searches.

If states are going to pursue a European model, they must take steps to improve that framework, shield small businesses from excessive regulatory burdens, and avoid foreseeable unintended consequences.

## FIGURE 1: PRINCIPLES FOR EFFECTIVE STATE DATA PRIVACY LAWS



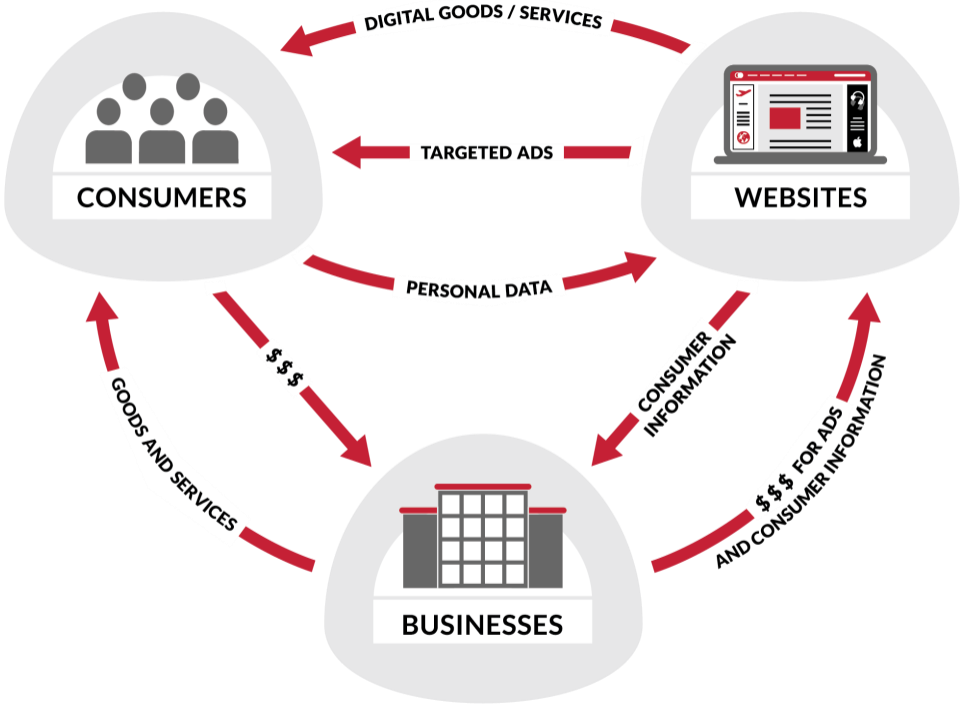
# UNDERSTANDING "AD-TECH" AND THE DATA PRIVACY PARADOX

At its core, data privacy protection involves trade-offs. Attempts to regulate data privacy fall short because people are not presented enough information to decide if the trade-offs are worthwhile.[1] All state data privacy models, for example, give consumers instruments that are too crude for making trade-off decisions, asking them to consent or do not consent to data collection, and delete or do not delete collected data.[2] These binary approaches are not nuanced and fail to account properly for context. Instead, they err by establishing constant and universal rights that create market inefficiencies and harms. Professor Helen Nissenbaum argues that the nature of online data privacy is less a matter of individual preferences and more contextually dependent on case-by-case decisions.[3] New data privacy laws should reflect that reality and tailor rules to specific contexts rather than broadly granting rights in all cases to either consumers or businesses. States looking to protect data privacy should improve upon America's traditional sector approach and craft narrow rules that promote free, efficient markets that are flexible enough to treat different types of data differently and in context.

Much of the data privacy debate has been created by the 21st century's shift toward online, internet-based commerce and trade. As shopping moves online, businesses advertise online. In exchange for free access to content, website creators and hosts collect consumer information—*e.g.*, purchasing patterns and browsing activity—that they then sell to businesses and advertisers so that ads can be targeted to likely consumers. Targeted advertising can yield better sales revenues and help businesses improve products and services. This new marketing model is known as the advertising technology (ad-tech) business model (Figure 2).

[1] Mike Masnick, **We're Bad at Regulating Privacy, Because We Don't Understand Privacy**, TechDirt, August 13, 2018.
[2] *Ibid.*
[3] Scott Berinato, "**Stop Thinking About Consent: It Isn't Possible and It Isn't Right**," *Harvard Business Review*, September 24, 2018.

## FIGURE 2: TARGETED ADVERTISING BUSINESS MODEL




Source: Federal Trade Commission

THE BUCKEYE INSTITUTE

Consumers have grown concerned, however, over how businesses use the information gleaned through the ad-tech model. A Cisco survey, for example, found that 86 percent of Americans care about data privacy and 79 percent of respondents were skeptical about sharing data because they are uncertain about how that data is used. Not surprisingly then, surveys show that Americans want Congress to protect their data privacy, with more than 80 percent of Democrats and Republicans supporting federal data privacy laws. And, according to the Pew Research Center, 81 percent of Americans believe the costs of data collection by private companies do not justify their perceived benefits.[4]

Despite these concerns, most Americans are generally unwilling to pay to protect their data—creating the "privacy paradox."[5] Panda Security found eight in 10

[4] Pew Research Center, **Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information**, November 15, 2019.
[5] Susanne Barth, "**The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review**," *Telematics and Informatics*, Volume 34, Issue 7 (November 2017) p. 1038-1058.

Americans said they valued their data more than keeping social media free to use, but more than seven in 10 respondents are not "willing to pay to protect their privacy."[6] Ajit Ghuman found that only half of U.S. consumers are willing to pay $8 per month for a fully private social media network.[7] Caleb Fuller found that 86 percent of respondents were not willing to pay anything for additional privacy protections when using Google.[8] Virtual private networks or VPNs create a layer of privacy between frequented websites and their internet service providers—but Americans seem unwilling to pay for that added protection either. According to NordVPN, a large VPN service provider, only 33 percent of Americans use a VPN,[9] and a Forbes market study found only 56 percent of those users actually pay for VPN access.[10] Fewer than one in five Americans are willing to pay anything to protect their privacy, and those who are willing to pay are not willing to pay much.[11]

Although reluctant to pay to protect easily accessible data that reveals little, Americans seem more concerned about protecting sensitive data like banking information, healthcare and biometric data, and insurance information.[12] A 2023 study finds consumers prioritize location, medical, and banking records the most. A Harvard Law study similarly found most Americans willing to pay only $5 per month for privacy but would demand $80 per month for companies to access personal data.[13] But here, too, context is important. Research from Professors Kirsten Martin and Helen Nissenbaum reveals that consumers care less about precise location markers like GPS coordinates than they do about less precise location information such as information about being near a hospital or in a certain store.[14] Capitalizing on emergent privacy laws that threaten to shrink information

---

[6] **8 in 10 Americans Say They Value Online Privacy—But Would They Pay to Protect It?**, Panda Security, September 11, 2021.

[7] Ajit Ghuman, **Research: A Market Where Consumers Can Pay for Privacy Is Emerging**, VentureBeat, April 30, 2021; Chris Teale, **Voters Overwhelmingly Back Major Provisions of Proposed Federal Data Privacy Law**, Morning Consult Pro, June 15, 2022.

[8] Caleb S. Fuller, "**Is the Market for Digital Privacy a Failure?**," *Public Choice*, 180 (2019), 353—381.

[9] Ema Globyte, **NordVPN Survey Shows: A Third of Americans Use a VPN**, NordVPN, June 28, 2023.

[10] Chauncey Crail, **VPN Statistics and Trends in 2023**, Forbes, February 9, 2023.

[11] Ben Walker, **How Much Does a VPN Cost? (And How to Save Money)**, All About Cookies, August 16, 2023.

[12] **Survey: Consumer Attitudes Towards Data Privacy**, IBM Newsroom (Last visited August 21, 2023).

[13] Anya Skatova, Rebecca McDonald, Sinong Ma, Carsten Maple, "**Unpacking Privacy: Valuation of Personal Data Protection**," *Plos One*, May 3, 2023. ; Angela G. Winegar and Cass R. Sunstein, **How Much Is Data Privacy Worth? A Preliminary Investigation**, *Journal of Consumer Policy*, Volume 42, Issue 425 (2019).

[14] Scott Berinato, "**Stop Thinking About Consent: It Isn't Possible and It Isn't Right**," *Harvard Business Review*, September 24, 2018; and Kirsten Martin and Helen Nissenbaum, "**What**

pools, some direct-to-consumer marketing companies now buy data from consumers for between $5 and $50 per month.[15] Similarly, Tapestri pays consumers $25 per month for location data from their cell phones—a higher monthly fee for more sensitive user information. When offered a costless privacy benefit, Americans want laws to protect privacy, but the strength of that desire—measured by how much they will pay—depends on the type of data being protected and what it reveals about them. Data privacy legislation should account for and reflect those differences.

**Is It About Location?**" *Berkeley Technology Law Journal*, Volume 35, Issue 251 (December 2019) p. 253-326.

[15] Tatum Hunter, **These Companies Will Pay You for Your Data. Is It a Good Deal?**, *The Washington Post*, February 6, 2023.

# EUROPEAN AND AMERICAN DATA PRIVACY REGIMES

The United States and the European Union (EU) have pursued different data privacy frameworks for decades. Burdened by past data collection abuses,[16] Europe generally pursues a rights-based privacy regime designed to enshrine the civil, political, social, and economic rights of European citizens. The United States has rejected Europe's approach in favor of a sector-specific policy that prioritizes limiting consumer harm.[17]

**U.S. Data Privacy Policy**

Contrary to popular suggestion, the United States does not have a hollow federal privacy system that provides little privacy protection for its citizens. In fact, the United States has numerous sector-specific data privacy laws at the state and federal levels that govern the collection, storage, and sharing of data in the financial, healthcare, and education sectors. The Health Insurance Portability and Accountability Act (HIPAA) fines unauthorized data transfers in healthcare, and the Fair Credit Reporting Act (FCRA) does the same for financial data.[18] The Gramm-Leach-Bliley Act (GLBA) regulates the collection and disclosure of sensitive financial data like credit history, bank account information, social security numbers, and income data; and requires privacy policy notices and security programs to protect financial data.[19] Education data, is protected under the Family Education Rights and Privacy Act (FERPA),[20] and the Children's Online Privacy Protection Act (COPPA) requires operators of online services that collect personal information to "notify users about the data collection, receive parental consent, and maintain 'reasonable procedures' to protect that data."[21] These sector-specific federal laws are in addition to state laws that police the use of

[16] Fredric D. Bellamy, **U.S. Data Privacy Laws to Enter New Era In 2023**, Reuters, January 12, 2023; Cristina Pop, **EU vs US: What Are the Differences Between Their Data Privacy Laws?**, Endpoint Protector, September 27, 2022.
[17] Fredric D. Bellamy, **U.S. Data Privacy Laws to Enter New Era in 2023**, Reuters, January 12, 2023.
[18] Will Rinehart, **The Law & Economics of "Owning Your Data"**, American Action Forum, April 10, 2018.
[19] Garry Kranz, **Gramm-Leach-Bliley Act (GLBA)**, TechTarget (Last visited August 21, 2023).
[20] **Family Educational Rights and Privacy Act (FERPA)**, U.S. Department of Education (Last visited August 21, 2023).
[21] Clare Y. Cho, **Challenges with Identifying Minors Online**, Congressional Research Service, March 23, 2023.

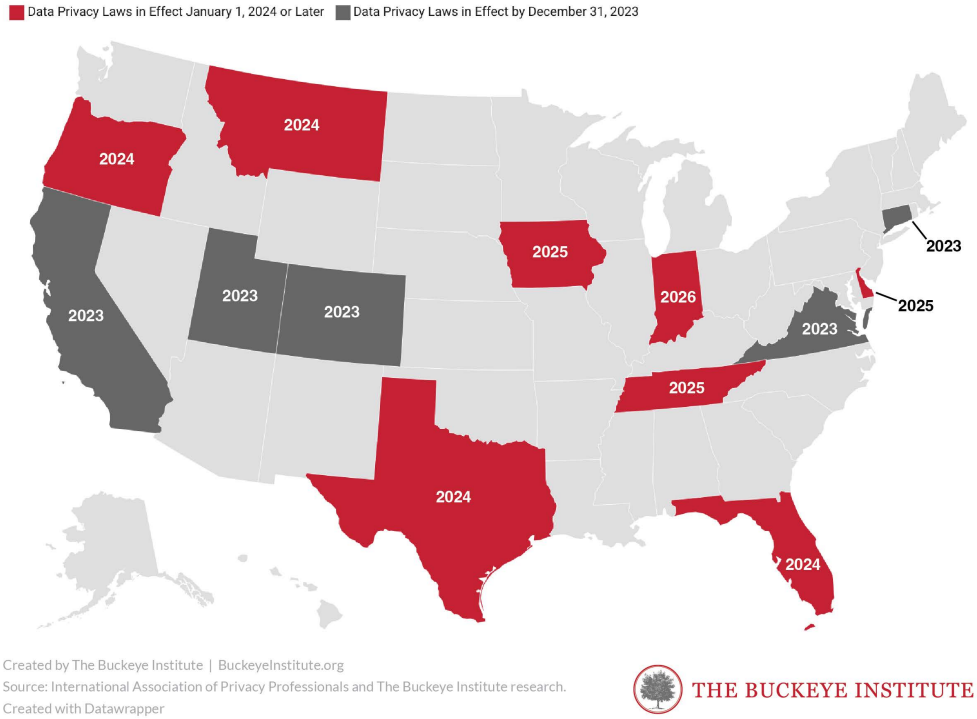
biometric data, promote data security and record disposal, and punish identity theft.[22]

And then there is the Federal Trade Commission (FTC), the "chief federal agency on privacy policy and enforcement since the 1970s," which prosecutes unfair and deceptive trade practices under Section 5 of the FTC Act.[23] As of 2020, the FTC had issued four of the 10 largest privacy fines worldwide, including a $3 billion fine against Facebook, which, until recently, was larger than all other global privacy fines combined.[24] The agency brings cases against social media businesses, advertising technology companies, and the mobile application ecosystem generally, including more than 130 spam and spyware cases, 80 general privacy lawsuits, and 80 cases against companies for inadequate data protection.[25]

[22] Noah Ramirez, **The Great Big List of Data Privacy Laws by State**, Osano, December 18, 2019; **2023 State Biometric Privacy Law Tracker**, Husch Blackwell (Last visited August 21, 2023); Geoff Scott, **Internet Privacy Laws in the US: A Guide to All 50 States**, Termly, September 10, 2018; **Data Security Laws**, National Conference of State Legislatures, May 29, 2019.
[23] **Protecting Consumer Privacy and Security**, Federal Trade Commission (Last visited August 21, 2023); and Chris Jay Hoofnagle, Woodrow Hartzog, and Daniel J. Solove, **The FTC Can Rise to the Privacy Challenge, But Not Without Help from Congress**, Brookings Institute, August 8, 2019.
[24] Kimball Dean Parker, **The Hidden Dangers of Privacy Laws Like the GDPR and CCPA**, Forbes, November 25, 2020.
[25] ***Federal Trade Commission 2020 Privacy and Data Security Update***, Federal Trade Commission, 2020.

**Figure 3: States with Comprehensive Data Privacy Laws**

As of September 29, 2023




Created by The Buckeye Institute | BuckeyeInstitute.org
Source: International Association of Privacy Professionals and The Buckeye Institute research.
Created with Datawrapper

THE BUCKEYE INSTITUTE

## The European Privacy Failure

By enacting the General Data Protection Regulation (GDPR), the Europe Union created a self-proclaimed "comprehensive" data privacy law that gives consumers the "right" to access, correct, and delete information at-will across all sectors and for businesses of all sizes.[26] Europe's rights-based approach pursues a once-size-fits all framework that mistakenly assigns a type of data right to something that cannot be owned. That approach has been a disaster from the start.

First, with its 99 articles, GDPR is complex and intentionally vague, which makes compliance expensive. Companies must spend a lot of time, money, and resources learning what they can and cannot do, and once they learn the appropriate course of action, they must then follow additional guidance from the European Data

[26] U.S. International Trade Administration, **European Union – Data Privacy and Protection** (Last visited September 14, 2023)

Protections Board and court rulings.[27] Constructing internal policies to ensure data is secure but accessible can be difficult.[28] To comply with GDPR, many companies must create additional data inventory and mapping to accommodate access and deletion requests, create consent management systems, and update their privacy policies, all of which must be routinely updated to accommodate new privacy rules.[29] And, to make it worse, GDPR is layered on privacy laws emerging in other states and countries that make complying with all of the rules all at once pricey and laborious. The International Association of Privacy Professionals (IAPP) and EY (formerly Ernst & Young) estimated Fortune 500 companies spent $16 million to comply with GDPR in the two years leading up to its effective data, while mid-sized firms "spent an average of $550,000."[30] A PricewaterhouseCoopers report found 88 percent of companies spent $1 million or more staying in compliance with GDPR, and 40 percent spent more the $10 million.[31] And Data Grails found that seven in 10 organization systems will not scale to stay in compliance with Europe's emergent data privacy regimes.[32] Once the law actually passed, more than a thousand news sites were "suddenly unavailable trying to visit the EU, with the bulk being smaller, local outlets," according to reporting from Gizmodo.[33]

Second, Europe's data privacy law digs protective regulatory moats around large technology companies that shield them from market competition, with one expert claiming "[b]ig companies like Facebook are 10 steps ahead of everyone else, and 100 steps ahead of regulators."[34] Large technology companies like Meta and Google have spent the human-time equivalent of hundreds of years and billions of dollars preparing for privacy legislation—an advantage over smaller firms with smaller profit margins and less staff.[35] Citing GDPR rules and using market leverage over websites reliant on their services, Google shifted the regulatory burden onto its

---

[27] Paul McCormack, **The Creeping Cost of Data Compliance**, Privitar, December 1, 2022; and Oliver Smith, **The GDPR Racket: Who's Making Money From This $9bn Business Shakedown**, *Forbes*, May 2, 2018.

[28] Paul McCormack, **The Creeping Cost of Data Compliance**, Privitar, December 1, 2022

[29] **The Age of Privacy: The Cost of Continuous Compliance**, DataGrail, May 2019.

[30] Ryan Khurana and Ryan Radia, ***European Union's General Data Protection Regulation and Lessons for U.S. Privacy Policy***, Competitive Enterprise Institute, May 18, 2018.

[31] Luke Irwin, **How Much Does GDPR Compliance Cost in 2023?**, IT Governance European blog, May 10, 2023.

[32] **The Age of Privacy: The Cost of Continuous Compliance**, DataGrail, May 2019.

[33] Spence Purnell, **Why Data Privacy Laws are Bad for Consumers**, *The Detroit News*, November 25, 2022.

[34] William Rinehart, **What Is the Cost of Privacy Legislation?**, The Center for Growth and Opportunity at Utah State University, November 17, 2022; and Jūra Liaukonytė, **X post**, February 19, 2022, 9:59 a.m.; and Mark Scott, Laurens Cerulus, and Steven Overly, **How Silicon Valley Gamed Europe's Privacy Rules**, Politico, May 22, 2019.

[35] Alex Moazed, **How GDPR is Helping Big Tech and Hurting Competition**, Applico (Last visited September 14, 2023).

advertisers by forcing them to collect affirmative consent to collect user data or lose access to the search engine for advertisements. Google also used the GDPR as justification to tweak the company's privacy settings, a change that would allegedly enable Google to siphon data from smaller advertising publishers that rely on the Google platform.[36] Google denies taking greater control of advertising publisher data,[37] but it is clear that GDPR has made less popular websites lose more traffic than popular websites, increasing market concentration.[38]

Third, GDPR negatively effects smaller firms, start-ups, and new innovators. [39] A 2022 study by three Oxford economists found that GDPR disproportionately impacted small businesses, caused exposed business profits to drop 8.1 percent, but had no effect on the profits or sales of large tech companies like Meta, Apple, and Google.[40] Startups and other small firms rely on angel and venture capital investment to fund initial investments to get the business off the ground. By limiting access to data, a key input to technological innovation, studies have shown that GDPR has reduced the total number of venture deals and cut capital investment by as much as half.[41] It has cost small, e-commerce websites nearly twice as much revenue as large firms.[42] Other studies show rights-based privacy laws raise compliance costs for all businesses while increasing regulatory uncertainty for businesses looking to invest in destinations with a firm regulatory hand.[43] In addition to imposing these costs, GDPR failed to adequately protect consumers and families, instead earning a reputation as the law that destroyed the

[36] Mark Scott, Laurens Cerulus, and Steven Overly, **How Silicon Valley Gamed Europe's Privacy Rules**, Politico, May 22, 2019.
[37] *Ibid.*
[38] Julia Schmitt, Klaus M. Miller, and Bernd Skiera, **The Impact of Privacy Laws on Online User Behavior**, Cornell University, October 19, 2021.
[39] Jian Jia, Ginger Zhe Jin, and Liad Wagman, "**The Short-Run Effects of the General Data Protections Regulation on Technology Venture Investment**," *Informs Pubs Online*, Volume 40, Issue 4 (March 1, 2021) p. 593-812.
[40] Chinchih Chen, Carl Benedikt Frey, and Giorgio Presidente, **Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally**, working paper, Oxford Martin School, University of Oxford, January 6, 2022.
[41] Jian Jia, Ginger Zhe Jin, and Liad Wagman, **The Short-Run Effects of GDPR on Technology Venture Investment**, working paper, National Bureau of Economic Research, November 2018.
[42] Samuel Goldberg, Garrett Johnson, and Scott Shriver, "**Regulating Privacy Online: An Economic Evaluation of the GDPR**", *American Economic Journal* (Publication Forthcoming).
[43] 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; and Castro, Luke Dascoli, and Gillian Diebold, ***The Looming Cost of a Patchwork of State Privacy Laws***, Information Technology and Innovation Foundation, January 24, 2022.

seamless user experience online by encouraging annoying, rapid-fire pop-ups and cookie notices.[44]

[44] Kate Fazzini, **Europe's Sweeping Privacy Rule Was Supposed to Change the Internet, but So Far It's Mostly Created Frustration for Users, Companies, and Regulators**, CNBC, May 5, 2019.

# PRINCIPLES FOR EFFECTIVE STATE DATA PRIVACY LAWS

America's federal data privacy system narrowly focuses on addressing actual privacy harms by design. Ideally, Congress would enact a preemptive federal data privacy standard that limits the enforcement power of federal agencies, eliminates the risk of a complex and burdensome web of data privacy laws, and builds on the existing sector-based harm-reduction approach to data privacy. But that has not happened, and the false perception that the United States has little privacy protection has tempted states to pursue their own regulatory data privacy regimes. Unable to preempt federal law, states are enacting data privacy rules that emulate the failed European approach over the traditional harm-prevention model (Figure 3).[45] That is a mistake.

Fortunately, by following several key data privacy principles, states can sidestep Europe's pitfalls and balance privacy protections with free markets. States looking to adopt their data privacy rules should prioritize an opt-out framework, narrowly tailor the scope of the law, and reassert free market principles. Data privacy legislation should not encourage businesses to collect more data to comply with the new rules. It should avoid abusable risk assessments and instead include an affirmative defense for complying with National Institute of Standards and Technology Standards (NIST) best practices. Enforcement authority should be vested in state attorneys general to avoid messy and frivolous private rights of action—but that authority should be limited and clearly defined so the law cannot be stretched beyond its original intent. Finally, government agents should need warrants to access collected data unless technology companies voluntarily share information without government coercion. States have followed these principles with varying degrees of success (Figure 4).

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

## FIGURE 4: STATE LAWS ADHERENCE TO DATA PRIVACY PRINCIPLES

| STATE LAWS | Adopted an Opt-Out Only-Approach | Narrowly Tailored Privacy Laws* | Allowed Flexible Pricing Models | Gave Discretion in Privacy Policies | Eliminated Data-Collection Mandates | Incentivized Best Practices | Prohibited Private Right of Action/ Frivolous Lawsuits | Kept Private Data Out of Gov't Hands |
|---|---|---|---|---|---|---|---|---|
| California Consumer Privacy Act | | | ✓ | | ✓ | | | |
| California Privacy Rights Act | | | ✓ | | ✓ | | | |
| Colorado Privacy Act | | | ✓ | | | | ✓ | |
| Connecticut Data Privacy Act | | | ✓ | | | | ✓ | |
| Delaware Personal Data Privacy Act | | | ✓ | | | | ✓ | |
| Florida Digital Bill of Rights Act | | | ✓ | | | | ✓ | |
| Indiana Consumer Data Protection Act | | ✓ | ✓ | | | | ✓ | |
| Iowa Consumer Data Protection Act | ✓ | ✓ | ✓ | | | | ✓ | |
| Montana Consumer Data Privacy Act | | | ✓ | | | | ✓ | |
| Oregon Consumer Privacy Act | | | ✓ | | | | ✓ | |
| Tennessee Information Protection Act | | ✓ | ✓ | | | | ✓ | |
| Texas Data Privacy and Security Act | | | ✓ | | | | ✓ | |
| Utah Consumer Privacy Act | ✓ | | ✓ | | | | ✓ | |
| Virginia Consumer Data Protection Act | | ✓ | ✓ | | | | ✓ | |

Created by The Buckeye Institute | BuckeyeInstitute.org

Source: International Association of Privacy Professionals and The Buckeye Institute research.

*Defined as a law with no revenue thresholds, a processing threshold of 100,000 or more consumers, and two-tiered broker threshold triggered by any minimum consumer benchmark and at least 50% of revenue from data sales. Exempts at least 12 of the standard 15 exemptions, must exempt de-identified data from applicability, prefer that pseudonymous data is exempted.

THE BUCKEYE INSTITUTE

### Grow the Online Economy by Adopting an Opt-Out Only Approach to Data Collection

The most significant difference between GDPR and U.S. policy is the "opt-in vs. opt-out" structure of the data collection and privacy. Under both methods, companies gain user consent to collect and use data. Opt-out systems assume implied consumer consent allowing companies to collect data unless a consumer invokes their right to not have their data collected. Opt-in systems shift that burden by requiring companies to gain affirmative consent from consumers before data collection.

Opt-in structures sound appealing but most states pursuing data privacy legislation are rejecting them—and with good reason. As Will Rinehart of the Center for Growth and Opportunity explains, opt-in regimes have three major drawbacks: 1) consumers have less information than companies, making their cost-benefit analysis inherently incomplete; 2) consumers will mistake government-mandated action for the company suggested policy, and therefore mistake government signals for market signals; and 3) forcing opt-in requirements will establish them as the status quo, which will be difficult to change.[46]

Critics of opt-out systems argue that because users know less about how the data is collected and used than those who collect that data, many users unknowingly agree to more data collection than they actually prefer.[47] But the private sector has notified users of opt-out rights before, and users have exercised those rights. Apple, for example, made it clear to app store participants that they could opt-out of tracking by online apps during Apple's iOS 14.5 software update in 2022. That notification sent tidal waves downstream to companies like Meta (formerly Facebook) that rely on Apple software to collect data across applications that they can then sell to advertisers. Within a day, Meta lost 26 percent of its stock value and about $10 billion.[48] Ninety-four percent of users opted out of data tracking after being prompted by a pop-up notification.[49] That was certain to be the case because even consumers who hardly value their data privacy would opt out of data collection if that selection cost them nothing. Any benefit at no perceived cost is a steal. The more important revelations in this case study are that data privacy laws have massive trade-offs and that there is a high cost to privacy protection.

As more consumers opt out of data collection, companies will have less information available to build effective market strategies, which will encourage companies to process even more data on those users that continue to trade their data for free website access. With less data, advertising becomes less targeted and less effective (Figure 5). With poor advertisement targeting, fewer people will likely spend money online because the online advertisements no longer effectively target their

---

[46] Will Rinehart and Allison Edwards, **Explaining the EU's General Data Protection Regulation**, American Action Forum, May 22, 2018.

[47] Jeff Sovern, "**Opting in, Opting out, Or No Options at All: The Fight for Control of Personal Information**," *Washington Law Review*, Volume 74, Number 4 (October 1, 1999).

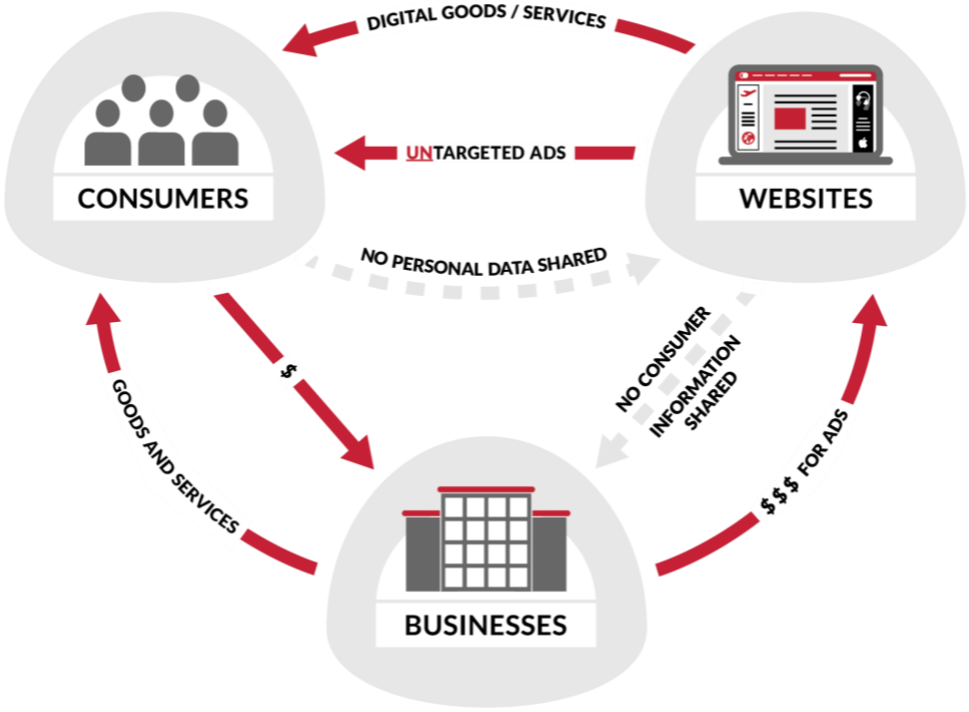
[48] Barbara Ortutay, **Meta, Formerly Facebook, Faces Historic Drop As Stock Tanks**, Associated Press, February 3, 2022; and Will Rinehart, **As If We Needed More Evidence There's a Privacy-competition Tradeoff**, The Exformation Newsletter, March 3, 2022.

[49] Naomi Nix, **Facebook Reports First-ever Decline in Revenue, Hinting at Darkening Economy**, *The Washington Post*, July 27, 2022; Greg Bensinger, **Americans Actually Want Privacy. Shocking.**, *The New York Times*, May 20, 2021.

desires.[50] As Rinehart notes, smaller firms that market direct-to-consumer (*i.e.*, that do not have brick-and-mortar stores or that use wholesalers or retailers) suffered the most since they use precision ads—reinforcing that even well-designed privacy rules often pinch the small competitors.[51]

States have mostly avoided opt-in frameworks, reserving them for more sensitive data types. Some states have adopted looser applications. California more broadly defines "personal information," making opt-in regimes to reign, and stretching those opt-in rights to other data types, such as biometric data and voice recordings.[52] Opt-out frameworks should replace opt-in requirements to avoid dismantling online competition and entrenching more successful businesses.

## FIGURE 5: UNTARGETED ADVERTISING BUSINESS MODEL




Source: Federal Trade Commission

THE BUCKEYE INSTITUTE

[50] Will Rinehart, **As If We Needed More Evidence There's a Privacy-competition Tradeoff**, The Exformation Newsletter, March 3, 2022; Eric Benjamin Seufert, **How Does IDFA Deprecation Impact Ad Prices?**, MDM Content, August 24, 2020.
[51] Will Rinehart, **As If We Needed More Evidence There's a Privacy-competition Tradeoff**, The Exformation Newsletter, March 3, 2022.
[52] David Stauss and Mike Summers, **How do the CPRA, CPA & VCDPA treat biometric information?**, ByteBackLaw.com, February 2, 2022.

**Protect Small Businesses by Narrowly Tailoring Data Privacy Laws**

The regulatory burdens of data privacy laws disproportionally fall on the shoulders of small businesses—reducing competition and increasing market concentration.[53] To protect small businesses, data privacy laws should be narrowly tailored in three ways: 1) appropriately adjusting revenue, processing, and broker thresholds; 2) exempting existing privacy laws; and 3) carefully defining terms and exempting certain types of data.

Learning from European failures, nearly all state data privacy laws build in financial benchmarks, like revenue, processing, or broker thresholds, to narrow the law's scope and shield small businesses from harm. Data privacy laws should apply primarily to businesses that rely heavily on collected consumer data. In this respect, minimum revenue thresholds are a poor proxy for setting the law's reach, and business revenue thresholds should be avoided. Subjecting businesses with high revenue volumes and thin profit margins to complicated, onerous regulatory requirements risks encouraging them to close and remove their value and productive capacity from the marketplace. Lawmakers looking to protect small businesses should instead tie any revenue benchmark to a provision under which the law only applies to businesses that meet a revenue trigger from the sale or collection of data *and* collect data from a minimum number of users, ideally 100,000 or more consumers for data processing or earning 50 percent of revenue from data sales.

Contending with a preexisting data privacy infrastructure, states attempting to universalize data privacy rights typically exempt a long list of laws that govern everything from health and financial records to education and employment information. Exemptions vary by state—but every state exempts some federal laws that govern healthcare, education, and financial records. Tennessee's law, for example, has an especially narrow scope that carves out most federal data privacy laws[54] and exempts government entities, nonprofit organizations, higher educational institutions, scientific research, insurance data, and motor vehicle records.[55] Following Tennessee's lead, state laws at least should exempt data already governed by federal law.

---

[53] Garrett A. Johnson, Scott K. Shriver, and Samuel G. Goldberg, ***Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR***, March 20, 2020.
[54] **Tennessee Information Protection Act**, S.B. 73, H.B. 1181, May 24, 2023.
[55] F. Paul Pittman, Abdul M. Hafiz, Yuhan Wang, **Tennessee Passes Comprehensive Data Privacy Law**, White & Case, June 23, 2023.

State data privacy legislation should also 1) clearly define the data subject to the law; 2) narrowly tailor those definitions to prevent expansion; and 3) require more protection for more sensitive data.[56] Americans value protecting their sensitive information—personally identifiable information, biometric data, health, and geo-location—more than de-identified or anonymized data.[57] Consumer correction and deletion rights should be reserved for sensitive data that can reasonably identify users if exposed, such as social security numbers or banking information. Florida, Iowa, and Tennessee similarly exempt pseudonymous data.[58] By keeping applicability thresholds high, exempting existing privacy structures, and structuring state laws to reflect American privacy concerns, state data privacy laws can remain narrow and effective.

### Allow Businesses to Develop Flexible Pricing Models

Because businesses purchase online consumer data to target advertisements to would-be customers more effectively, new data privacy rights that allow consumers to access and delete personal data will shrink information pools and force businesses to raise prices, run lower quality ads, or redesign business models. Consumers can invoke those rights on a case-by-case basis, and businesses should be permitted to do so as well. Most states allow prices to change for legitimate business reasons. Some data privacy advocates call for states to remove these market-friendly provisions and instead mandate that all consumers be treated the same.[59] But that would create a classic free-rider problem by allowing those who do not pay for services through dollars or data to still reap the benefits of low-cost online services.[60]

Businesses use prices to match their goods and services to the needs and wants of their customers. Disallowing price adjustments to reflect consumer preferences, data privacy laws would encourage consumers to overuse free deletion rights, which would decrease advertising effectiveness and increase data processing on consumers who continue to exchange their data for website access.[61] With no prices

---

[56] ***Consumer Data Privacy Guiding Principles & Legislative Checklist***, Reason Foundation.
[57] *Ibid*.
[58] Katherine Danko, **Comparing U.S. Comprehensive State Privacy Laws: Treatment of Pseudonymous Data**, Network Advertising Initiative, August 14, 2023.
[59] Adam Schwartz, **The Payoff from California's "Data Dividend" Must Be Stronger Privacy Laws**, Electronic Frontier Foundation, February 15, 2019.
[60] Ashley Johnson, **Florida Privacy Bill Is Bad For Business and Consumers**, Information Technology & Innovation Foundation, May 3, 2023.
[61] **Protecting Internet Data Privacy Without Hindering Innovation Requires a Dose of Legislative Humility & a Strong Trust in Consumer Intelligence**, Libertarianism.org, October 26, 2018.

to guide business decisions, needed feedback on how businesses can improve their services to meet consumer desires goes unnoticed, degrading the overall consumer experience online.[62] Data privacy laws should make clear that prices can fluctuate to meet market demand on a case-by-case basis and let consumers bear the consequences of their actions. Failing to let prices fluctuate leads to lower quality services, businesses sponsor fewer advertisements, websites raise prices on everyone, and advertisers and websites risk permanently closed operations. States should resist binding constraints on prices, a highly valuable market signal.

### Give Businesses Discretion in Notifying Consumers of Privacy Policies

The best methods for businesses to communicate data privacy policies vary by setting. Traditional websites, online applications, operating systems, and offline loyalty programs all differ in appropriate privacy notice design—but data privacy laws rigidly enumerate how businesses must notify consumers. The average data privacy policy is more than 4,000 words, takes 16 minutes to read, and is often difficult to understand.[63] This is because data privacy notices are written for other lawyers, not consumers, in an effort to inoculate businesses from lawsuits. Data privacy policies themselves are rarely unique, often outsourced to vendors that simply copy other legal formulas.[64]

The ineffectiveness of data privacy policies has not stopped states from mandating them or specifying must be disclosed. Data privacy laws push governments into the user experience and user interface (UX/UI) by not only requiring data privacy policies, but also detailing how consumers must be notified. A better approach would give businesses incentives and flexibility to offer privacy notices in different ways, such as easy-to-follow videos instead of complicated legal addendums.[65] States emulating European data privacy law require affirmative consumer consent before collecting data, which spawns recurring pop-up notifications and website banners that destroy the user's online experience.[66] California complicates this further by requiring data collection companies to notify users of privacy options before or at the point of data collection. Businesses under California's privacy law must post a "Do Not Sell or Share My Personal Information" link on their websites,

---

[62] *Ibid.*

[63] Jarni Blakkarly and Daniel Graham, P**rivacy Policy Comparison Reveals Half Have Poor Readability**, Choice.com.au, January 28, 2022.

[64] **What Is Privacy UX?**, UserTesting.com (Last visited September 5, 2023).

[65] *Ibid.*

[66] Jon Healey, **What are those annoying website popups about cookies? And what should you do about them?**, *Los Angeles Times*, September 1, 2021.

creating more pop-ups and further cluttering smaller devices.[67] Consumer data privacy preferences would be improved if businesses have discretion regarding notification and consistent guidance across states on how best to present privacy options to consumers.

## Protect Against Data Breaches by Eliminating Data-Collection Mandates

Poorly designed consumer rights-based privacy laws unintentionally encourage more sensitive data collection, not less. Lamenting the "new privacy circle of hell," Alistair Barr of Bloomberg explains how a simple request to access and delete personal information for one website under California's data privacy law can quickly involve sharing personal information with vendors that request names, email addresses, personal pictures, driver's license information, signatures, and home addresses.[68] Attempts to protect, access, and delete consumer information can ironically perpetuate a vicious cycle in which more information is collected and at risk. In May 2018, for example, a hacker accessed tech executive Jean Yang's Spotify account and used it to invoke GDPR's access rights to obtain her home address, credit card information, and music history.[69] The more data that is collected to comply with data privacy laws, the more sensitive information there is for hackers to access, retrieve, and expose.[70]

Every state already regulates how industry must respond to data breaches,[71] but data privacy laws should be designed to reduce their likelihood. Privacy laws generally do this through "data minimization" provisions that limit data collection to what is adequate and necessary, but those protections are insufficient and can even lead to conflicting rules across different laws.[72] The Ohio Personal Privacy

---

[67] **California Consumer Privacy Act (CCPA)**, California Attorney General's Office, May 10, 2023.

[68] Alistair Barr, **Come on a Trip into the New Privacy Circle of Hell**, Bloomberg, January 9, 2020.

[69] Kashmir Hill, **Want Your Personal Data? Hand over More Please**, *The New York Times*, January 15, 2020; James Pavur, Casey Knerr, ***GDPArrrrr: Using Privacy Laws to Steal Identities***, Blackhat USA, 2019; Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax, Flanders Make, Wim Lamotte, Ken Andries, **Personal Information Leakage by Abusing the GDPR 'Right of Access'**, Usenix Association, 2019.

[70] **What Is an Attack Surface?**, Avast Business (Last visited September 5, 2023).

[71] **Security Breach Notification Laws**, National Conference of State Legislatures, January 17, 2022.

[72] B. Stephanie Siegmann and Emily M. Covey, **Expanded U.S. State Privacy Laws in Six States Bring Increased Data Privacy Requirements and Significant Risk of Class Action Suits and Enforcement Actions**, Hinckley Allen, April 5, 2023; and Jennifer Huddleston, **The**

Act—although unenacted—exemplifies how to limit the risk of data breaches. The bill instructs businesses not to "collect personal data that it would not otherwise collect in the ordinary course of business," not to "retain personal data for longer than it otherwise would retain such data," and allows companies to redact personal information in their responses to consumers, thus decreasing potential hacker entry points and safeguarding consumers.[73] That antidote is not perfect, nor is it without costs. Failing to collect some personal information may make it impossible to comply with certain requests, increase data omission in correspondence, and even risk court battles. On the economic side, data minimization requirements reduce access to input data, harming technological innovation in fields like 5G and artificial intelligence.[74] Not every unintended consequence can be averted, but limiting the legislation's scope can help forestall some economic fallout. As Thomas Sowell famously proclaimed, there are no solutions, only trade-offs[75]—and Ohio's bill balances those trade-offs better than most.

### Incentivize Best Practices, Don't Mandate Risk Assessments

Most states require businesses that process sensitive information to create data protection impact assessments to weigh the risks and benefits of using data in different settings. Risk assessments help organizations understand the value of privacy in specific contexts and introduce alternative methods of data protection. Most states confine the assessments to targeted advertising, the sale of data, and sensitive activities posing a "heightened risk of harm," but those terms are often ill-defined and unclear.[76] States should clarify those provisions and define terms carefully.

Instead of requiring businesses to create impact assessments, states should encourage businesses to adopt risk assessments—as well as generally agreed upon privacy protection best practices—by giving organizations an affirmative defense. Namely, if a regulated business shows its policies comply with privacy recommendations detailed by the National Institute of Standards and Technology

**Consequences of Regulation: How GDPR is Preventing AI**, Cato at Liberty blog, June 22, 2023.

[73] Logan Kolas, ***The Buckeye Institute: Ohio Personal Privacy Act, Among Best in the Nation, Could Be Even Better***, The Buckeye Institute, February 2, 2022.

[74] Nicholas Martin, Christian Matt, Crispin Niebel, and Knut Blind, "**How Data Protection Regulation Affects Startup Innovation**," *Information Systems Frontiers*, Volume 21, p. 1307—1324 (2019).

[75] Thomas Sowell, *A Conflict of Visions: Ideological Origins of the Political Struggles* (Basic Books, 2007).

[76] **Comparing the Data Protection Assessment Requirements Across the Next Generation of U.S. State Privacy Laws**, Bryan Cave Leighton Paisner, November 30, 2021.

(NIST), that business will have met its legal obligation. The voluntary NIST framework is more likely to be used if it provides compliant organizations with an affirmative defense in court. Following suggested industry best practices promotes flexibility and innovation to keep pace with technology trends while prioritizing privacy protections.[77]

A NIST-based best-practices affirmative defense provision promotes privacy protection in two ways. First, because NIST regularly updates its privacy framework, businesses will have the incentive to continually update their privacy protocols, too, rather than simply comply with data privacy laws that quickly become obsolete. Second, the NIST standards would provide an interstate framework for privacy protections across the country and help synchronize the patchwork of state laws that threatens to cost between $98 and $112 billion each year.[78] Importantly, states can pursue this provision—scaled to fit unique business models and risk profiles—alongside other efforts to pass and improve their own privacy laws.[79]

### Safeguard Responsible Businesses from Frivolous Lawsuits

Some fear too many legislative carveouts will leave consumers exposed—but the far bigger threat is an unmanageable data privacy regime stretched beyond its original intent.[80] California's data privacy regime provides a cautionary example. California's data privacy law grants the state attorney general broad discretion to expand the scope of the California Consumer Privacy Act.[81] Then-California Attorney General Xavier Becerra used that discretion to extend disclosure obligations, impose additional data privacy rules, and further regulate verification procedures and offline retailers.[82] Instead of passing an amendment to extend or make permanent exemptions for data in an employment or commercial context, California let those provisions expire—expanding the CCPA's scope by exposing

[77] **NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0**, National Institute of Standards and Technology, January 16, 2020.
[78] 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.
[79] National Institute of Standards and Technology, **NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management**, Version 1.0, United States Department of Commerce, January 16, 2020.
[80] James Dempsey, **Exceptions in New US State Privacy Laws Leave Data Without Security Coverage**, International Association of Privacy Professionals, May 17, 2022.
[81] Perkins Cole, **Recent Developments At the California Attorney General's Office Concerning the CCPA and Enforcement**, LexBlog, July 27, 2021.
[82] Philip R. Recht and Jeffrey P. Taft, **California Attorney General Releases Proposed Regulations for the CCPA**, Mayer Brown, October 16, 2019.

businesses to prosecutorial "sweeps" for everything from mobile applications to loyalty programs to employee data.[83]

To avoid repeating these mistakes, states should limit executive power by clearly defining enforcement rules. Investing this power in state attorneys general avoids messy, expensive, and often frivolous lawsuits that can deter investment and innovation. Private rights of action are included in many privacy laws, including the Illinois Biometric Information Privacy Act (BIPA), which has been a disaster.[84] In January 2019, the Illinois Supreme Court ruled individuals can be aggrieved under BIPA even if they suffer no harm—inspiring hundreds of lawsuits, empowering lawyers, chilling technological innovation and business formation, and diverting millions of dollars to the plaintiffs' bar.[85] Private rights of action encourage class action lawsuits that often do more to hurt businesses than help the aggrieved individuals. Less than 10 percent of class members claim anything at all, and when they do receive payment, claimants often receive coupons of questionable value, rather than cash settlements.[86] Attorney general enforcement is not perfect, but so long as states can effectively limit executive branch mission creep, it is better than inviting messy private rights of action.

**Keep Data out of Government Hands**

All state consumer data privacy laws currently exempt government entities—and for good reason. Allowing individuals to request state government access and delete government-controlled data could muddy police and regulatory investigations. To quell fears over technology companies giving consumer data to the government, states should explicitly prohibit government agencies from collecting consumer and personal data from technology companies without a subpoena or warrant. Similar provisions will not prevent companies from turning over data that they reasonably believe will prevent imminent harm to an individual, nor would these provisions prohibit governments from collecting publicly available data, but they would shield consumers from intrusive government actions.

---

[83] Avi Gesser, Tricia Bozyk Sherno, Johanna Skrzypczyk, and Michael R. Roberts, **CCPA Will Cover Employee and B2B Bata—Amendments Fail to Pass**, Debevoise & Plimpton, September 2, 2022; and Connor Krindle and Amy Patton, **Employers Beware—Attorney General Announces Sweeps Targeting Employee Data**, JD Supra, July 25, 2023.

[84] ***Ill-Suited Privacy Rights of Action and Privacy Claims***, Institute for Legal Reform, July 2019.

[85] *Ibid.*

[86] ***Consumers and Class Actions: A Retrospective and Analysis of Settlement Campaigns***, Federal Trade Commission, September 2019.

State and federal governments routinely dodge Fourth Amendment privacy protections by simply purchasing personal data from data brokers without a warrant. Although the U.S. Constitution prohibits state and federal agencies from forcing companies to turn over data, it does not prohibit them from purchasing that data. Some members of Congress have introduced legislation to curb federal intelligence and law enforcement agencies' authority to purchase data from data controllers, but those bills remain unenacted.[87] At the state level, only California has protected consumers from overly aggressive government entities by requiring business auditors to secure a warrant to access personal information. That's a good first step, but even that provision does not prevent law enforcement or government agencies from asking for access or purchasing the data outright.

Governments have a poor data security track-record. Sensitive data stored by the Louisiana Office of Motor Vehicles, for example, was exposed when hackers breached third-party data transfer service, MOVEit.[88] Ohio has an unfortunate history of healthcare data breaches,[89] and Ohio Medicaid providers suffered a data breach as recently as 2021.[90] At the federal level, ProPublica notoriously used feloniously leaked or breached IRS tax data to supposedly expose how little America's wealthy pay in taxes. That story was much ado about nothing but highlighted the need for governments to examine and amend privacy rules to safeguard their own data more effectively.[91] State data privacy laws would do well to limit law enforcement and government agencies from collecting or storing consumer data without a warrant.

---

[87] David B. McGarry, **Congress Must Close This Fourth Amendment Loophole**, *The Hill*, August 3, 2023.

[88] Bennett Roland, Jr., **Breaking Down the Massive Hack that Exposed Louisiana OMV Data**, KALB.com, June 16, 2023; James Finn, **Massive Software Hack Exposes Most Louisianans' OMV Data**, Nola.com, June 15, 2023.

[89] **The Biggest Health Care Data Breaches You Should Know About in Ohio**, Fox8.com, August 4, 2023

[90] Kaitlin Schroeder, **Ohio Medicaid Providers' Data May Have Been Exposed from Data Breach**, *Dayton Daily News*, June 22, 2021.

[91] Jesse Eisinger, Jeff Ernsthausen, and Paul Kiel, **The Secret IRS Files: Trove of Never-BeforeSeen Records Reveal How the Wealthiest Avoid Income Tax**, ProPublica, June 8, 2021.

# Conclusion

Data privacy protection requires tradeoffs and flexibility. One-size-fits-all solutions like those modeled in Europe are doomed to fail. Unfortunately, in the absence of comprehensive federal data privacy legislation, U.S. states have pursued their own versions of Europe's failed model. Although not ideal, states that do opt for data privacy laws should follow several key principles to mitigate unintended consequences and harmful results. States should prioritize opt-out frameworks, protect small businesses with narrow data privacy scopes, encourage market incentives in privacy policy, and clearly define and limit the enforcement powers of executive agencies. Taking these steps will not ensure no poor outcomes, but they will strike a more appropriate balance between Europe's all-or-nothing privacy regime and America's free-market approach designed to limit consumer harms. America should resist following Europe's broken data privacy model or at least make it better.

# 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 state and local taxes, state-level budgets, technology and innovation policy, and labor market issues.

Kolas has conducted state-level tax modeling and budget research for states such as Iowa, Louisiana, New Hampshire, and North Carolina. He has authored policy papers, book chapters, blog posts, and op-eds on restoring Ohio's technology and innovation leadership, the effects of federal and state labor market policies on work, and on modernizing Ohio's outdated economic system to return the Buckeye State to economic prosperity and leadership. He is the author of The Buckeye Institute's three-part "Policies for More Innovation" series where he authored the reports ***A Policy Primer for Emerging Technology in Ohio*** and ***Modernizing Ohio's Policies to Seize New Economic Opportunities***. Kolas has also conducted **multiple analyses** estimating the number of state-level jobs lost to a $15 per hour minimum wage.

Kolas has testified to legislative committees on free-market policy and privacy issues. His commentary has been published by *The Columbus Dispatch*, *The Cincinnati Enquirer*, *Crain's Cleveland Business*, *The Lima News*, *St. Louis Post Dispatch*, Daily Signal, and the Foundation for Economic Education, amongst others.

Prior to joining Buckeye, Kolas was a research associate at the Herbert A. Stiefel Center for Trade Policy Studies at the Cato Institute, where his research focused on how employment is impacted by international trade, the effect of international trade taxes on state and federal government policies, and the regulatory burden imposed by government on American businesses and families.

Kolas is a native of Cincinnati and throughout his career has focused on researching Ohio-related policies. He earned his Bachelor of Science in economics and political science from **George Washington University** and holds a Master of Science in applied economics from the **University of Maryland**.

**Acknowledgements**

The author would like to thank Amanda Latta, research and administrative assistant at The Buckeye Institute, for her excellent research assistance.

*Key Principles for State Data Privacy Laws*

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