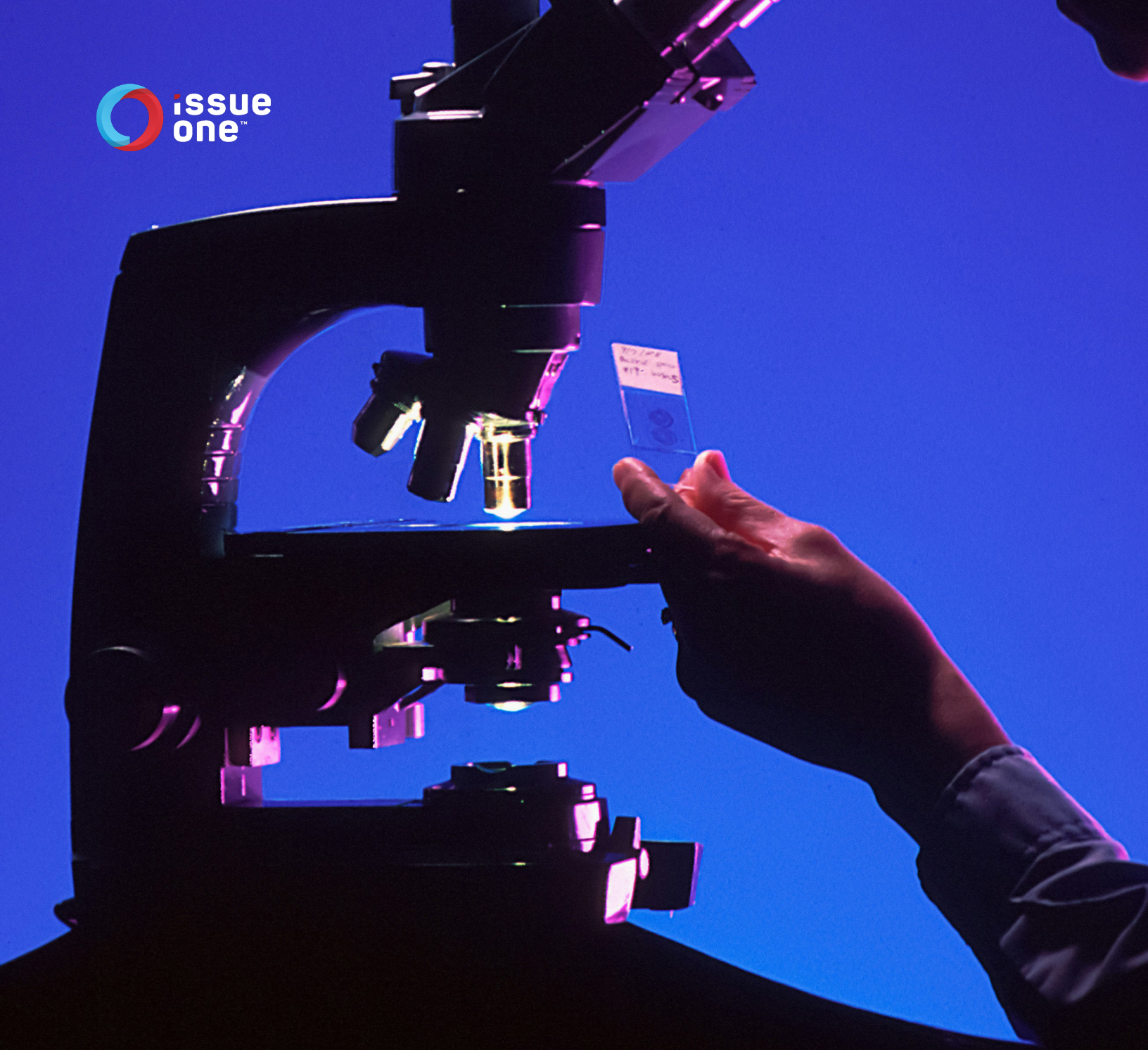


LABORATORIES OF CAPTURE

How the Tech Lobby Shapes State Data Privacy Laws

Ellen Zeng, Liana Keesing & Isabel Sunderland

CONTENTS

EXECUTIVE SUMMARY

With Congress deadlocked on privacy legislation, statehouses have become the front line of data privacy policymaking. But instead of producing strong protections, many states have adopted laws shaped heavily by the technology industry. These laws appear protective while preserving companies' ability to collect, infer, and monetize personal data at scale.

This report examines seven states — **Washington, Virginia, Connecticut, Alaska, Utah, Montana, and Maine** — and shows how major tech firms and their affiliated coalitions have used a consistent strategy to steer privacy laws toward a weak national standard.

The first part of that strategy is drafting the bills themselves. Lobbyists routinely supply full bill text and "technical" amendments that closely resemble the Virginia Consumer Data Protection Act, an industry-friendly model with no private right of action, narrow definitions of sensitive data, and attorney-general-only enforcement. And when lawmakers introduce stronger privacy-protective proposals, the industry works behind the scenes to reshape them. When stronger bills gain momentum, multiple competing alternatives suddenly appear, overwhelming limited staff capacity and dividing political support. Alongside these procedural tactics, the industry deploys a network of proxy groups that present corporate positions as neutral expertise: trade associations, think tanks, multi-industry coalitions, and "small business" alliances. State chambers of commerce and associations often echo talking points handed to them by the tech-funded U.S. Chamber of Commerce, giving national lobbying campaigns a local voice.

The seven case studies reveal how this playbook operates in practice. In Virginia, an Amazon lobbyist drafted the bill that became the industry's preferred template. In Connecticut, a strong bill was steadily weakened after coordinated opposition from tech and healthcare coalitions. In Alaska and Utah, lobbyists overwhelmed small, part-time legislatures with minimal staff. Similar and related tactics were leveraged in Washington, Montana, and Maine, with varying success.

The negative consequences are significant. Weak state privacy laws leave children vulnerable to algorithmic profiling, allow data brokers to continue selling sensitive information to foreign nations, and fuel opaque AI systems that shape what people see, know, and believe. These are not just privacy harms — they affect public health, national security, and democratic participation.

Yet this trajectory is not inevitable. Lawmakers in several states have begun to resist the industry's model, and public awareness is growing. This report offers recommendations for various stakeholders, arguing that strong privacy laws require strong processes: transparency about who writes the bills, limits on industry's role in drafting them, and meaningful enforcement mechanisms. The rules governing the data economy must be written in public, for the public — not by the companies that profit from our personal lives.

1. INTRODUCTION

In the United States, the rules that govern how companies collect and exploit personal data have not been written in Congress or by federal regulators. They have been shaped, quietly and incrementally, in statehouses. As federal efforts to pass comprehensive privacy legislation stalled, the technology industry turned to a more fragmented and more manageable arena: state legislatures with short sessions, limited staff, and little in-house technical expertise. There, companies and their trade groups have worked systematically to design, promote, and normalize a weak model of privacy law that preserves their ability to collect and monetize data at scale.

This report documents how that strategy works in practice. Drawing on lobbying disclosures, hearing testimony, and bill text from seven states — ***Washington, Virginia, Connecticut, Montana, Alaska, Utah, and Maine*** — it shows how industry actors:

- Provide pre-drafted bill language and "technical" amendments that set the terms of debate;
- Flood legislatures with competing, industry-friendly bills when stronger proposals emerge;
- Present corporate-funded coalitions as neutral experts and small-business advocates; and
- Use these tools to entrench the "Virginia model," a framework that appears protective while leaving the surveillance economy largely intact.

The stakes extend far beyond any single state. Because privacy laws spread by imitation, a weak framework in one legislature can quickly become the default standard across the country — and the template for future federal legislation. The result is a data economy in which companies face few real limits on how much information they can collect, how long they can keep it, or how they can deploy it in advertising, AI systems, or political messaging.

The sections that follow explain how we reached this point, why statehouses are so vulnerable to industry capture, and how the same playbook recurs across the country with remarkable consistency.

1.1 The Data Economy

Over the past two decades, personal data has become a central input of the modern economy. Search engines, social networks, mobile apps, online retailers, and advertising intermediaries all depend on the same underlying model: collect as much information as possible about individuals, infer as much as possible from that information, and monetize those profiles through targeting, optimization, and behavioral prediction.

This model extends far beyond what people knowingly share. Companies track browsing histories, app usage, device identifiers, precise location, search queries, purchase records, and social networks. Data brokers aggregate and sell this information, creating detailed dossiers that can be used for advertising, risk scoring, political outreach, and more. Increasingly, these same datasets feed into AI systems that personalize content,

recommendations, and search results.

For dominant technology firms, this is not a side business; it is the business. Their revenues depend on the ability to observe and influence people at scale. Any law that significantly limits collection, restricts the use of sensitive data, or allows meaningful enforcement threatens the foundation of this model. That basic conflict — between rights-protective privacy law and a commercial system built on surveillance — defines the politics of data privacy in the United States.

1.2 The Federal Policy Vacuum

Despite repeated warnings from researchers, advocates, and regulators, Congress has not created a comprehensive federal framework to govern the data economy. Today, most commercial data practices are regulated only by a patchwork of sector-specific laws and general consumer protection authority.

The ***Children's Online Privacy Protection Act (COPPA)***, enacted in 1998, remains the only major federal privacy statute focused on online data collection. It predates smartphones, social media, and modern targeted advertising. COPPA offers some protections for children under 13 but excludes teenagers, relies heavily on parental consent mechanisms that companies have learned to route around, and was never designed for today's platform-dominated environment.

Attempts to pass broader federal privacy legislation have repeatedly stalled. The ***American Data Privacy and Protection Act (ADPPA)*** advanced further than any previous effort, winning bipartisan support and clearing a House committee in 2022. The ***American Privacy Rights Act (APRA)*** followed in 2024, again reflecting serious bipartisan negotiation. Both efforts, however, collapsed amid disagreements over enforcement, preemption of state laws, and the scope of individual rights — disagreements sharpened and amplified by industry lobbying.

Within a federal vacuum, Big Tech turned to a new arena of influence: the statehouse.

1.3 The Rise of State Power

As Congress failed to act, states stepped in. Beginning with the California Consumer Privacy Act (CCPA) in 2018, legislatures across the country introduced bills to define basic rights over personal data and obligations for companies that collect it. Since then, nearly twenty states have enacted some form of comprehensive privacy statute.

State lawmakers did not start from scratch. They borrowed concepts, definitions, and structures from existing laws — first from Europe's General Data Protection Regulation (GDPR) and the CCPA, and later from newer state models like Virginia and Connecticut. In theory, this kind of policy diffusion can accelerate good ideas. In practice, whoever controls the initial templates and offers the most "help" with drafting exerts outsized influence over what spreads.

This cycle of replication has turned statehouses into ideal targets for industry influence. Unlike Congress, most state legislatures operate with skeletal staff, short sessions, and scarce in-house technical expertise. A single aide may be responsible for analyzing hundreds

of bills in a session, leaving little room for independent research. That vacuum is quickly filled by outside "experts" offering pre-drafted bill language and policy guidance — and this dependence gives corporations and industry-funded coalitions a direct path to shape the law.

This report does not attempt to define an ideal privacy law in detail, but a few concepts are essential to understanding the case studies that follow in Section 3. Strong privacy laws place substantive limits on data collection, treat privacy as a default right rather than a series of opt-outs, and ensure meaningful enforcement (often through both public agencies and private rights of action). Weaker, industry-backed models generally do the opposite: they preserve broad data-collection permissions, rely on narrow definitions of sensitive data, and restrict enforcement to a single overburdened agency. These differences shape the debates in every state discussed in this report.

When lawmakers set out to draft privacy legislation, they rarely begin with a blank page. The technology industry arrives first — armed with bill text, suggested amendments, talking points, and a network of organizations prepared to frame these proposals as the "consensus" model for consumer protection.

Across dozens of states, the same patterns repeat. The companies that profit from collecting and monetizing personal data have developed a sophisticated playbook for shaping the rules intended to govern them. This playbook does not rely on blocking legislation outright. Instead, it focuses on defining what "privacy law" means in practice: narrow consumer rights, broad data-collection permissions, and minimal accountability.

A central part of this strategy is locking in a single template. Since 2021, that template has been the ***Virginia Consumer Data Protection Act (CDPA)***, the first law drafted largely with industry input and designed to be easily replicated in other states. Its structure favors business needs: no private right of action, attorney-general-only enforcement, broad exemptions, narrow definitions of sensitive data, and a default of "opt out" rather than genuine limits on collection. Much of the playbook is aimed at ensuring that this model — not rights-protective alternatives — becomes the standard other states adopt.

2. OVERVIEW

Inside the Industry Playbook

2.1 Main Tactics in the Playbook

Write the Bills

Industry lobbyists and their outside counsel frequently draft full bills or key sections, presenting them as technical "best practices." Across states, these drafts often mirror the Virginia model almost word-for-word. When lawmakers are pressed for time or lack staff capacity, the industry version becomes the starting point — and, often, the final product.

Control the Amendments

Even when lawmakers introduce stronger bills, the industry works behind the scenes to reshape them. Lobbyists propose "technical fixes," offer redlines, and request late-stage clarifications that narrow definitions, expand exemptions, weaken enforcement, or turn

prohibitions into opt-outs. These changes systematically strip the bill of provisions that would push it beyond the Virginia model.

Flood the Zone

When a strong privacy proposal gains traction, the industry rarely confronts it head-on. Instead, it creates competition. Multiple alternative bills — usually modeled on the Virginia framework — are introduced simultaneously. This overwhelms legislative staff, divides advocacy coalitions, and creates political pressure to settle on the "compromise" version. That compromise is almost always the industry-backed version that resembles Virginia.

Use Proxy Groups to Launder Corporate Positions

Tech firms rarely testify under their own names. Instead, they rely on trade associations, think tanks, chambers of commerce, and coalitions that appear independent but share the same corporate funders. These organizations testify in hearings, publish white papers, and brief legislators under names implying independence, or emphasizing "consumer empowerment," "innovation," or "harmonization." In reality, many of these organizations are bankrolled by the very companies whose data practices they claim to be holding accountable.

Leverage Local Businesses as Political Cover

In many states, especially rural or conservative ones, national tech lobbyists amplify their message through hand-picked local business leaders. These individuals repeat talking points drafted by national coalitions: concerns about compliance burdens, the threat of "patchwork" regulation, or fears of litigation. Their involvement gives engineers of the Virginia model a local voice, helping lawmakers justify choosing weaker protections as the "pro-business" route.

2.2 The Players Behind the Playbook

Most state legislators never hear directly from Meta, Google, Amazon, or major data brokers. Instead they encounter a network of intermediaries that present themselves as experts, conveners, or protectors of innovation and small business.
These organizations fall into three broad categories:

- ***Multi-Industry Coalitions:*** Groups like the State Privacy and Security Coalition (SPSC) coordinate across dozens of companies — from tech giants to telecoms, insurers, data brokers, retailers, and advertisers. They often draft the bills and negotiate amendments on behalf of their members.

- ***Tech-Funded Trade Associations:*** TechNet, the Computer & Communications Industry Association (CCIA), NetChoice, and similar groups represent major platforms and advance their policy preferences across statehouses nationwide.

- ***Advocacy and Consumer Groups with Industry Ties:*** Think tanks, civil-society organizations, and "small business" alliances often receive funding from the same platforms they appear to independently critique. They help validate the Virginia model as reasonable and consumer-friendly, while casting stronger bills as unrealistic or harmful.

Multi-Industry Coalitions	*Advocacy and Lobbying Groups with Big Tech Ties*	*Trade Associations Representing Big Tech*
State Privacy and Security Coalition Multi-industry coalition of members including Amazon, Comcast, Google, Meta, NetChoice, and TechNet.	**Connected Commerce Council** Coalition framed for small business interests but receives support from Amazon, Facebook, and Google.	**TechNet** Trade association for tech execs and CEOs whose members include Apple, Amazon, Google.
Software Alliance Trade group of business software companies whose members include IBM, Microsoft, and Oracle, Software.	**Chamber of Progress** Nonprofit lobbying group that has backing from Apple, Google, Amazon, and Meta and was formed by a former Google lobbyist.	**NetChoice** Trade association representing technology firms including Amazon, Google, Meta.
Information Industry Association Trade association dedicated to the entertainment, consumer and business software industries. Members include Apple, Meta, Google, Amazon, etc.	**Consumer Technology Association** Lobbying group representing more than 2,000 tech companies whose members include Google, Facebook, Amazon, Airbnb, Lyft, etc.	**Computer & Communications Industry Association** Members represent communications and technology firms including Apple, Google, Amazon
Alliance for Automotive Innovation Trade association and lobby group whose members include international car and truck manufacturers.	**Consumer Data Industry Association** Lobbying group whose members include Amazon, Facebook, Google, Uber, etc.	**Internet Association** Google, Facebook, and Amazon were members of the now disbanded Internet Association.
	Future of Privacy Forum Advocacy group that receives funding from Big Tech companies such as Amazon, Google, Meta, Microsoft.	**Entertainment Software Association** Trade association representing the video game industry.
	TechFreedom Think tank that receives funding from Big Tech companies such as Google.	**Charter Communications** Spectrum's broadband connectivity company and cable operator.

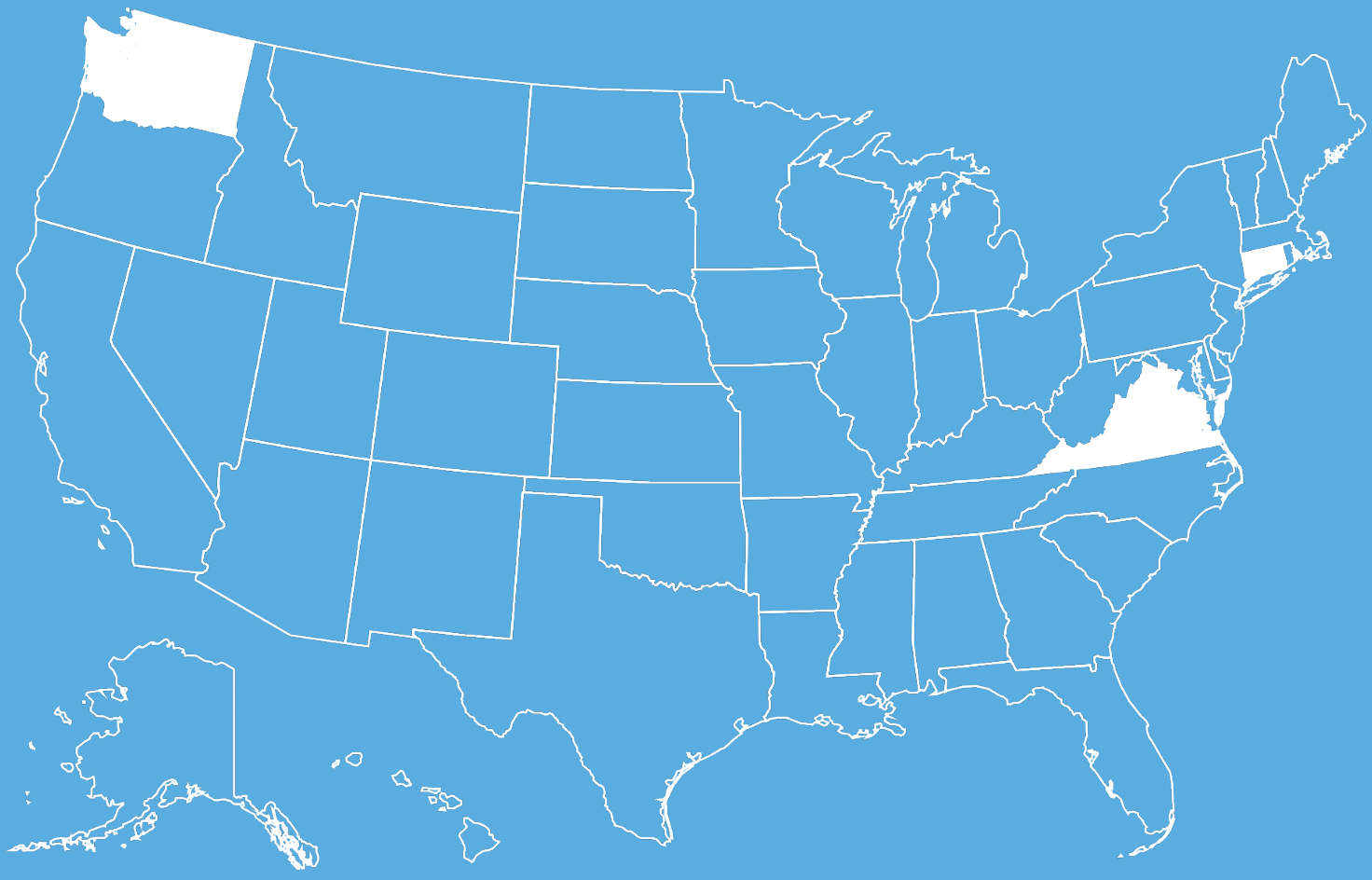
3. CASE STUDIES

How the Playbook Works in Practice

3.1 Building the Industry Model

The first phase of the tech industry's state-level strategy was to build a privacy framework that preserved the data economy while appearing to protect consumers. This model took shape through a series of early state experiments in Washington, Virginia, and Connecticut, where lobbyists translated the language of Europe's General Data Protection Regulation (GDPR) into a business-friendly form.

By 2021, the industry had solidified the Virginia model containing no private right of action, attorney-general-only enforcement, narrow definitions of "sensitive data," and broad exemptions for data collection. These early states became laboratories of capture, where industry influence was refined, normalized, and exported nationwide.



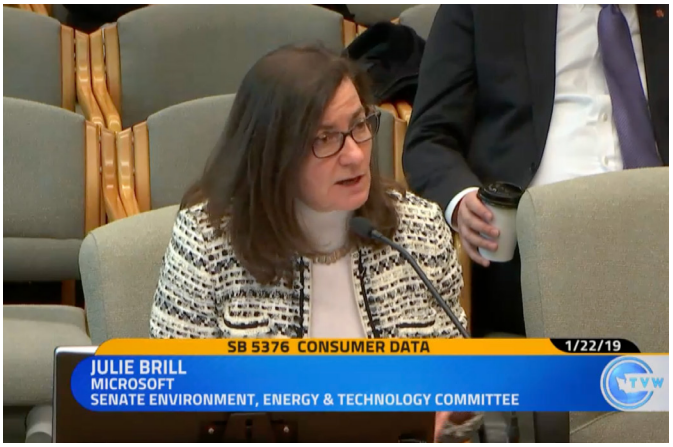
Case Study 1: Washington

Co-opting the legislative process **Flooding the zone**

Lobbying in Washington in 2019:

Amazon	Amazon spent $2.3 million on lobbying in 2019 – an increase of 547% from what it spent in 2018. Amazon hired 4 more lobbyists in 2019.
Microsoft	Microsoft spent slightly over $1 million on lobbying in 2019 – an increase of 158.52% from what it spent in 2018.
Apple	Apple spent $52,500 on lobbying in 2019 – an increase of 4,453% from what it spent in 2018.
Comcast	Comcast spent $273,774 on lobbying in 2019 – an increase of 42% from what it spent in 2018.
The Internet Association	The Internet Association spent $126,887 on lobbying in 2018 – an increase of 1005% from what it spent in 2017. The Internet Association hired 3 more lobbyists in 2017.
The Entertainment Software Association	The Entertainment Software Associate spent $104,403 on lobbying in 2019 – an increase of 31% from what it spent in 2018.

The ***Washington Privacy Act of 2019*** (SB 5376) marked the tech industry's initial attempt at codifying a favorable privacy model. SB 5376 was introduced January 30, 2019 based on the European Union's GDPR. However, tech industry lobbyists eventually carved out broad exemptions and narrowed its consumer rights. The bill died three months later on April 17.



Microsoft led the industry's push. Microsoft's President Brad Smith personally called state legislators to win support for the bill, Ryan Harkins, a senior policy director at Microsoft, annotated the final legislative draft and crossed out sections he deemed unsatisfactory, and Chief Privacy Officer Julie Brill testified in favor of the bill. Overall, Microsoft drastically increased its lobbying expenditure in Olympia from approximately $389,000 in 2018 to over $1 million in 2019, marking a 158.52% increase.

During the Senate Environment, Energy & Technology committee hearing on SB 5376, Alex Aleben, Washington State's Chief Privacy Officer said the bill's goal was "not to disrupt business, but to allow business to operate as usual with consumer protections," signaling that

the bill would impose few real constraints on big tech companies. And although the Attorney General's Office testified in favor of a private right of action, lawmakers ultimately left that provision out.

Though SB 5376 failed, Washington's bill laid the groundwork for the Virginia privacy model, later embraced by the tech industry as its preferred standard.

Washington Case Study Methodology

This research used lobbying disclosure data available on Washington's Public Disclosure Commission website. Because the Washington Privacy Act of 2019 was introduced in early 2019, spending was compared across 2018 and 2019 to capture changes in lobbying activity before and after the bill's introduction.

Hearing quotes were found by watching public hearing testimony available on the Washington State Legislature Website. Selected quotes were pulled from the Senate Environment, Energy and Technology committee hearing held on January 22, 2019, accessible by this link.

Case Study 2: Virginia

Co-opting the legislative process | **Flooding the zone** | **Portraying industry-funded groups as neutral**

Lobbying in Virginia in 2021:

Amazon	Amazon employed lobbyist Meade Spoots of Spotts Fain Consulting to introduce the Virginia bill. Amazon spent $319,954 on lobbying from May 2019-April 2021, including $144,000 on Spotts Fain Consulting. Amazon employed 9 lobbyists from May 2020-April 2021, picking up PJ Hoffman as privacy lead on Amazon's public policy team, and added a new outside lobbying firm, Two Capitols Consulting.
Google	Google employed 6 lobbyists from May 2020-April 2021, and added a new outside lobbying firm, McGuireWoods.

Virginia's Consumer Data Protection Act (HB 2307/ SB 1392) became the industry data privacy standard. Introduced on January 20, 2021, the bill sped through Virginia's short 26-day legislative session, passed both chambers by March 2, and took effect January 1, 2023.

Amazon led the lobbying charge in Richmond. The Virginia text was written by Amazon's contract lobbyist, Meade Spoots, and handed to sponsor Sen. Marsden. Between the 2019-20 and 2020-21 cycles Amazon alone reported $320,000 in lobbying expenses, and its political donations in Virginia ballooned from $27,750 in 2016 to $277,500 in 2020.

Alongside Google and Microsoft, the three tech giants registered 17 lobbyists during the 2021 session, up from 12 in the previous cycle. The U.S. Chamber of Commerce was also involved, with the Chamber's privacy working group president Jordan Crenshaw registered as a lobbyist to support the bill.

During a Senate committee hearing on the bill, Senator Marsden introduced Stacey Gray of the Future of Privacy Forum (FPF) as a data privacy expert "not advocating for any position or any industry." He noted that FPF took funding from the Robert Wood Johnson Foundation, along with "some corporate funding."

What he failed to mention was that Amazon referred Marsden to the Future of Privacy Forum, and disclosed to him that it financed the nonprofit.

Nevertheless, Gray was positioned as a trustworthy "phone-a-friend," able to

Future of Privacy Forum (FPF)

The Future of Privacy Forum is a Washington, D.C.–based think tank and advocacy organization that presents itself as a neutral convener of privacy experts bridging industry, academia, and policymakers. In practice, it operates as a leading industry-backed policy forum shaping the national conversation on data governance. FPF's corporate membership includes major technology and telecommunications companies such as AT&T, Comcast, Google, Meta (Facebook), Amazon, and Microsoft, along with financial and advertising firms whose business models depend on large-scale data processing.

answer technical questions and reinforce the bill's credibility during the hearing.
The industry's influence over SB 1392 was thinly veiled. However, it was still framed publicly as neutral, expert-driven policy advice. In the same committee hearing, Marsden said he had "calls with dozens of stakeholders" and entertained "all kinds of amendments" to meet business needs. Microsoft's senior public policy director Ryan Harkins and Amazon's policy manager Bill Way both testified in support of the bill, describing data privacy as essential to rebuilding trust in technology., Way specifically praised the bill for making Virginia "a leader in consumer privacy," masking how thoroughly the measure was aligned with Amazon's corporate interests.

By drafting the bill, saturating Richmond with lobbyists, and validating the effort through a seemingly neutral ally, Big Tech created a standard that the tech industry now advances in other states — and hopes to enshrine at the federal level.

Virginia Case Study Methodology

This research used lobbying disclosure data available on the Virginia Public Access Project (VPAP) website. Because Virginia's Consumer Data Protection Act was introduced in early 2021, lobbying spending was compared across 2020 and 2021 to capture changes in lobbying activity before and after the bill's introduction.

Hearing quotes were found by watching public hearing testimony available on the Virginia Senate Granicus platform. Selected quotes were pulled from the Virginia Senate General Laws and Technology committee hearing held on January 27, 2021, accessible by this link.

Case Study 3: Connecticut

Co-opting the legislative process

Flooding the zone

Portraying industry-funded groups as neutral

Weaponizing local businesses

Lobbying in Connecticut in 2021:

Google	Google spent $133,455.86 on lobbying from 2021-22 – a 35.49% increase from 2019-20.
Amazon	Amazon spent $191,058.50 on lobbying from 2021-22 – a 64.81% increase from 2019-20.
Meta	Meta spent $158,173.16 on lobbying from 2021-22 – a 23.94% increase from 2019-20.
TechNet	TechNet spent $26,250.00 on lobbying from 2021-22 – up from $0 in 2019-20.
The State of Privacy and Security Coalition	The State Privacy and Security Coalition spent $4,055.50 on lobbying from 2021-22, up from $0 in 2019-20.

In 2020, Senate Majority Leader Bob Duff introduced the consumer data privacy bill, which included a private right of action. At a public hearing on the bill, Duff described that the room was "filled with every single lobbyist [he's] ever known in Hartford," hired by the tech lobby to defeat his bill.

Duff reintroduced a revised version of his data privacy bill (SB 893) in 2021, but it too died in committee following strong opposition from industry-aligned groups like TechNet and the Software Alliance, as well as associations representing hospital networks, automakers, and retailers.

The healthcare sector was especially well represented in opposition, with the Connecticut Association of Health Plans, Connecticut Hospital Association, American Health Insurance Plan-Con all submitting testimony against the bill. In one instance, lobbyists claimed Senator Duff that his bill could harm data collection during public health emergencies.

In 2022, a new privacy bill finally passed in Connecticut, but in a much weaker form. Senator James Maroney, who sponsored the successful legislation, acknowledged that the final language was a compromise shaped in conversation with Andrew Kingman of the State Privacy and Security Coalition (SPSC). The result was the Connecticut Data Privacy Act, which closely mirrored the Virginia model and has since been replicated in several other states.

Although the bill received temporary support from some privacy advocates, that support was limited. Justin Brookman of Consumer Reports clarified that the organization only backed the Connecticut law to prevent an even weaker version from passing. However, Kingman

continues to pitch Connecticut's bill as a "consumer-friendly" model.

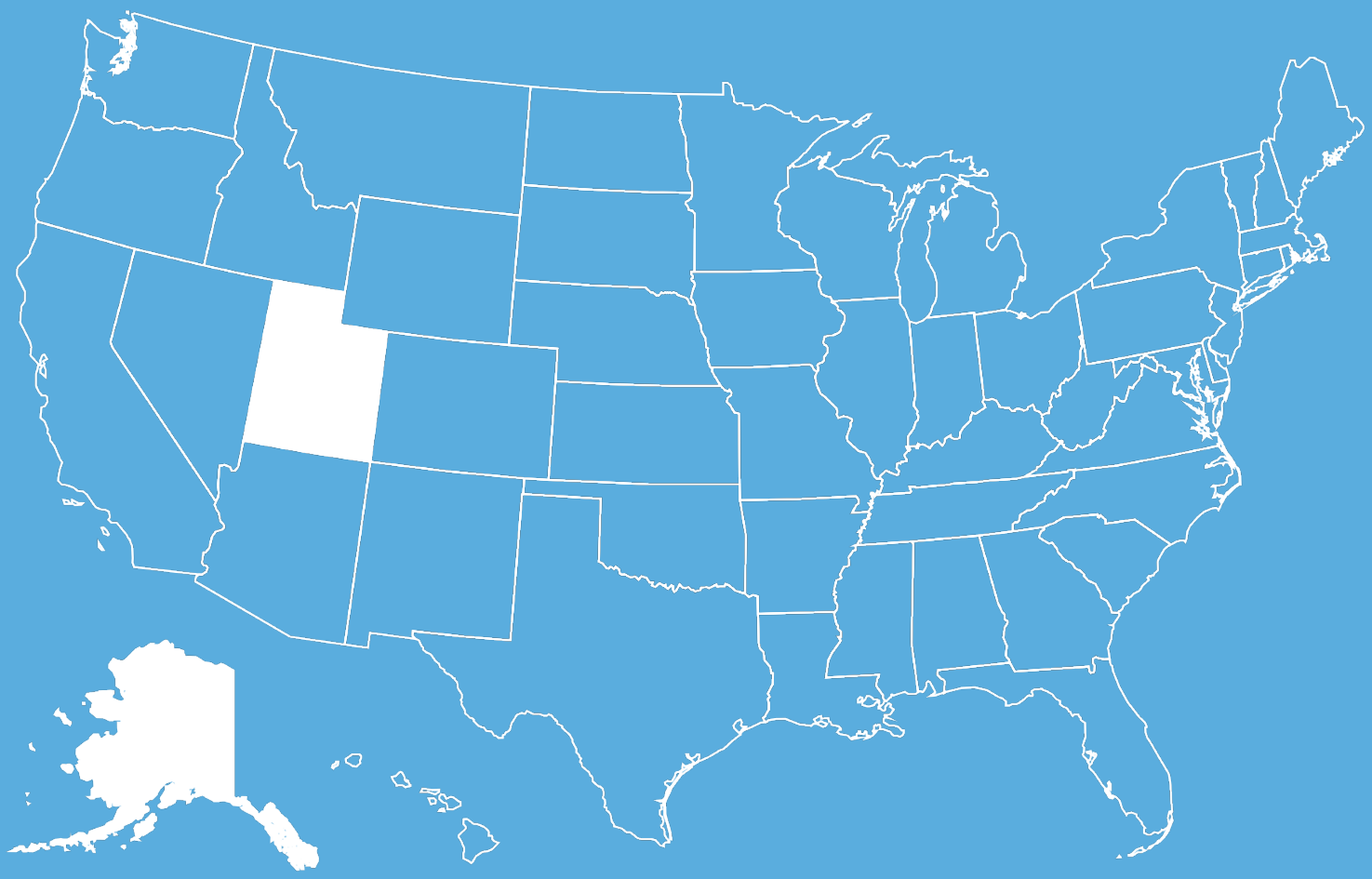
Connecticut's experience shows how persistent and consistent lobbying can shape legislation into something the industry finds acceptable. The final law passed, but in a very different form originally envisioned.

Connecticut Case Study Methodology

This research used lobbying disclosure data available on the Connecticut Office of State Ethics Lobbying website. Because the Connecticut Consumer Data Bill of Rights was introduced in early 2021, lobbying spending was compared from 2021-22 and 2019-20 to capture changes in lobbying activity before and after the bill's introduction.

3.2 The Playbook in Red States

The tech industry's influence is most visible in more conservative, rural, and remote states. Lawmakers in these states often serve part-time with limited staff resources, meaning industry lobbyists from Washington D.C. face little organized resistance to shape the legislative process. In this section, Alaska and Utah show how this strategy operates in practice, demonstrating how Big Tech can dominate even the smallest political arenas to secure policy laws that serve its interests.



Case Study 4: Alaska

Co-opting the legislative process | **Flooding the zone** | **Portraying industry-funded groups as neutral**

Lobbying in Alaska in 2022:

Amazon	Amazon spent $40,000 on lobbying in the 2022-23 session – an increase of 50% from what it spent during the 2021-22 session. They registered a lobbyist in the state for the first time in 2021 for "Matters relating to data management."
Meta	Meta spent $60,000 on lobbying in the 2022-23 session. They registered a lobbyist in the state for the first time in 2022 for "Matters related to data privacy and information technology."
TechNet	TechNet spent $23,328 on lobbying in the 2022-23 session. They registered a lobbyist in the state for the first time in 2021 for "Data privacy" among other lobbying.
The Consumer Technology Association	The Consumer Technology Association spent $10,500 on lobbying in the 2022-23 session. They registered a lobbyist in the state for the first time in 2022 for "Matters relating to consumer technology."

The Alaska Consumer Data Privacy Act (HB 159) became a clear example of how the tech lobby quietly suffocates privacy legislation in more rural, remote states, where legislative resources are limited and external influence often lands with disproportionate force. Introduced in 2021 and again in 2022, HB 159 aimed to grant Alaskans greater control over their personal data, with stronger enforcement than the industry-favored Virginia model. But as the bill moved through House committees, the tech industry quickly mobilized.

By January 2022, the tech lobby had landed in the state. During a House Labor & Commerce Committee hearing, an entire roster of industry representatives testified in opposition. Speakers represented the Entertainment Software Association, the State Privacy and Security Coalition (SPSC), the Computer & Communications Industry Association (CCIA), and TechNet.

The tech industry's goal wasn't to kill HB 159, but instead, to direct

ROBERT WOODY
American Property Casualty Insurers Association (APCIA)
Washington, D.C.
POSITION STATEMENT: Testified during the hearing on HB 159.

MAYA MCKENZIE, Technology Policy Council
Entertainment Software Association
Birmingham, Alabama
POSITION STATEMENT: Testified in opposition to HB 159.

ANTON VAN SEVENTER, Council
State Privacy and Security Coalition
Washington, D.C.
POSITION STATEMENT: Testified in opposition to HB 159.

ALYSSA DOOM
Computer & Communications Industry Association(CCPIA)
Washington, D.C.
POSITION STATEMENT: Testified in opposition to HB 159.

DAVID EDMONSON, Vice President of State Policy and Government Relations
TechNet
Austin, Texas
POSITION STATEMENT: Testified in opposition to HB 159.

it back to the Virginia industry model. Previously in 2021, Alaska legislators had received letters from industry groups urging them to adopt the Virginia Consumer Data Protection Act (VCDPA).

The most damning moment for HB 159 came in March 2022: Microsoft's Senior Director of Public Policy, Ryan Harkins, testified for the entirety of the House Judiciary Committee meeting and delivered a 30-minute PowerPoint presentation about data privacy.

He was positioned as an expert in data privacy to answer legislators' questions, such as about the inclusion of pseudonymous data and private rights of action, despite his entrenchment in industry interests. The bill did not advance any further.

The presentation underscored how deeply embedded the tech industry had become in the policy process. The tech lobby don't just oppose legislation; they co-opt the conversation. For lawmakers in other states, Alaska serves as a cautionary tale: even without passing a bill, the tech industry can still win.

Alaska Case Study Methodology

This research used lobbying disclosure data available on Alaska's APOC Online Reports platform which is maintained by the Alaska Public Offices Commission. Lobbying expenditures were found under "Employer of Lobbyist Summary," while lobbying registrations were found under "Lobbyist Registration Filings." Search terms in the footnotes were used to find results for specific technology firms. Because the Alaska Consumer Data Privacy Act (HB 159) was reintroduced in early 2022, lobbying spending was compared across 2021 and 2022 to capture changes in lobbying activity before and after the bill's introduction.

Hearing quotes were found by watching public hearing testimony available on the Alaska State Legislature website, which are all linked on the bill's page. The House Judiciary Committee hearing held on March 18th, 2022 is accessible by this link.

Case Study 5: Utah

Co-opting the legislative process | **Flooding the zone** | **Portraying industry-funded groups as neutral**

Lobbying in Utah in 2022:

Google	Google added 12 new lobbyists during the 2021 and 2022 sessions, 6 each respectively.
Amazon	Amazon added 2 new lobbyists in 2021.
Meta	Meta added 2 new lobbyists in 2022.
Apple	Apple added 2 new lobbyists in 2022.
NetChoice	NetChoice added 1 new lobbyist in 2022.
The Internet Association	The Internet Association added 2 new lobbyists in 2021.

Utah's 2022 Consumer Privacy Act (S.B. 227) is regarded as one of the weakest data privacy laws in the country. With its limited scope, lack of enforcement, and narrowly drawn definitions, the law ultimately serves industry interests more than consumer protections. Introduced on February 25, 2022, the bill moved through Utah's legislature in less than a month and was signed into law by March 24.

Senator Kirk Cullimore, the bill's sponsor, openly acknowledged the bill's industry influence. At the Senate Revenue and Taxation Committee public hearing introducing the bill, Cullimore stated the legislation had "a lot of input" from business interests after being delayed from a prior session.

Indeed, the final text of the bill was developed with Anton van Seventer, a lobbyist for the State Privacy and Security Coalition (SPSC), who was introduced as counsel. During the same committee hearing, Van Seventer positioned the SPSC as an "in-the-weeds advisor" for state-level data privacy legislation, claiming this experience gave him insight into other states' mistakes. Specifically, he portrayed S.B. 227 as a pragmatic alternative to California's stronger privacy laws, which he said cost the state billions of dollars in compliance costs and drove businesses out of the state. He explicitly stated his hope that the Utah model would be adopted in other states and eventually at the federal level.

Dylan Hoffman, Executive Director of TechNet at the time, also testified, but for no more than 30 seconds. He simply stated he wanted to align his comments with "his colleague Anton," not so subtly nodding at the existing relationship between the two tech organizations. Meanwhile, local business groups also legitimized the bill. President Dave Davis of the Utah Retail Merchants Association stated he ordinarily wouldn't be speaking in favor of more government regulations, but praised the bill for balancing consumer rights with business interests.

S.B. 227 illustrates how Big Tech can influence legislation by embedding itself in the legislative process and positioning its lobbyists as neutral experts, distanced from industry influence.

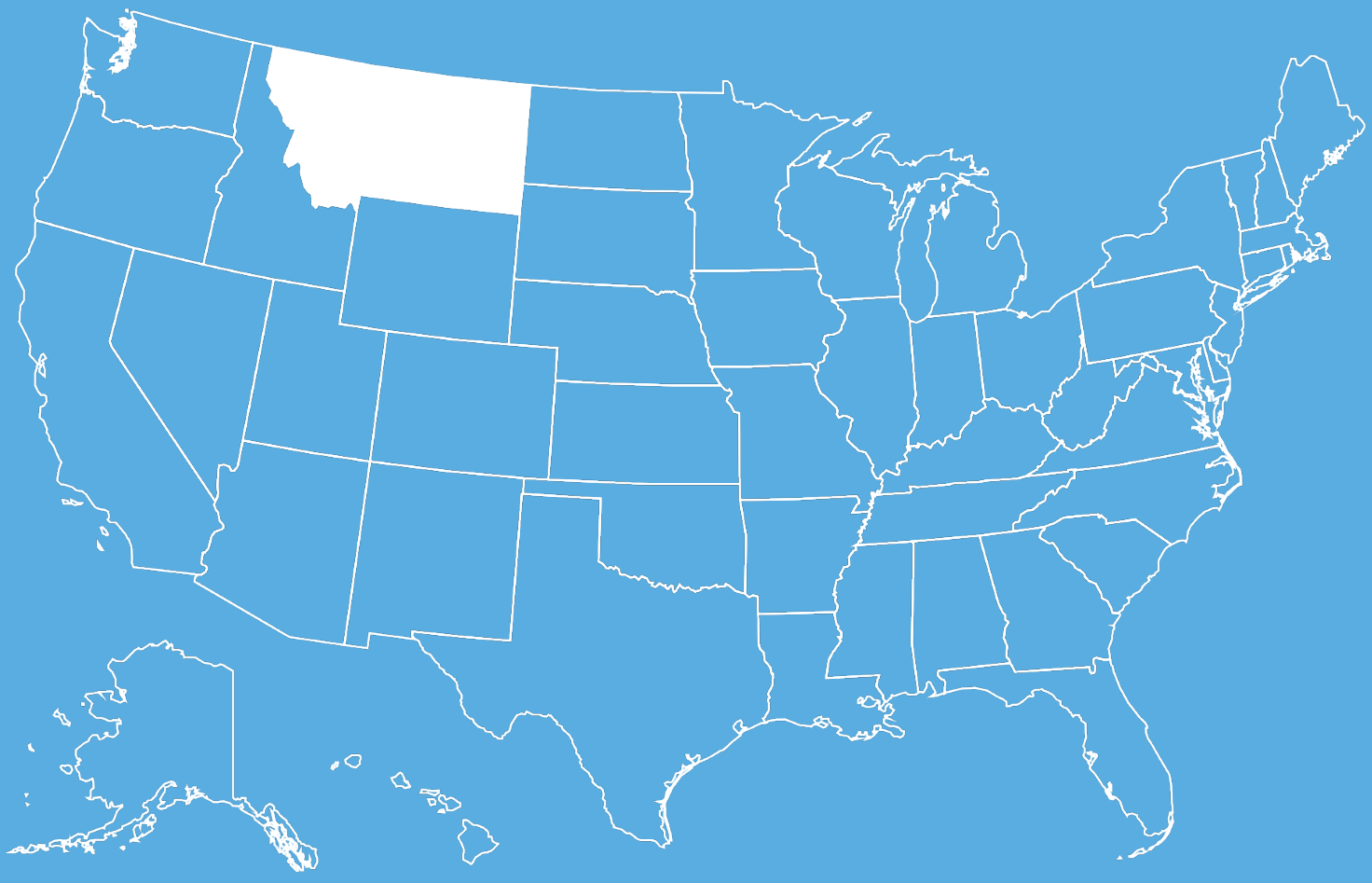
Utah Case Study Methodology

This research used lobbying disclosure data available on the State of Utah Financial Disclosures platform, which is maintained by the Utah Lieutenant Governor's Office. Utah lobbying disclosures do not include spending expenditures. Lobbyist registrations were found under "Lobbyist lookup by Principal Organization." Search terms in the footnotes were used to find results for specific technology firms. Because the Utah 2022 Consumer Privacy Act (S.B. 227) was reintroduced in early 2022, lobbying spending was compared across 2021 and 2022 to capture changes in lobbying activity before and after the bill's introduction.

Hearing quotes were found by watching public hearing testimony available on the Utah State Legislature website. The Senate Revenue and Taxation Committee hearing held on February 23, 2022 is accessible by this link.

3.3 Cracks in the Playbook

Montana marked a rare break in the tech lobby's campaign to control state privacy laws. In a state with a small, part-time legislature and limited staff, the technology industry expected an easy win. Lobbyists insisted on the legislature abandoning the Connecticut model – despite championing it in Maryland three months later. A Montana lawmaker called out this hypocrisy, highlighting how industry lobbyists tailor their message in each state, despite publicly denouncing the "patchwork" of privacy laws.



Case Study 6: Montana

Co-opting the legislative process | **Flooding the zone** | **Portraying industry-funded groups as neutral**

Lobbying in Montana in 2023:

Google	Google spent $39,410.68 on lobbying in 2023-24 session - an increase from $0 spent during the 2021-22 session.
Microsoft	Microsoft spent $40,000 on lobbying in the 2023-24 session – an increase of 19,000% from what it spent during the 2021-22 session.
Meta	Meta spent $26,000 on lobbying in the 2023-24 session – an increase of 78.21% from what it spent during the 2021-22 session.
The Technology Network	The Technology Network spent $30,144 on lobbying in the 2023-24 session – an increase from $0 spent during the 2021-22 session.
State Privacy and Security Coalition	State Privacy and Security Coalition (SPSC) registered for the first time in Montana during the 2023-24 session.

Montana's 2023 Consumer Data Privacy Act (SB 384) exposes a key contradiction in the tech lobby's national strategy: while industry groups routinely criticize the patchwork of data privacy laws, they simultaneously tailor their positions depending on where they're lobbying. Senator Daniel Zolnikov, a Republican who had unsuccessfully attempted a stronger privacy bill in 2019, reintroduced legislation on February 16, 2023. His goal was to craft a law based on Connecticut's stronger data privacy model and establish a standard for red states. But the tech lobby quickly mobilized in response.

The most influential broker was Andrew Kingman of the State Privacy and Security Coalition (SPSC). While publicly praising the draft as a sensible and balanced approach to consumer privacy in a committee hearing, Kingman privately urged Sen. Zolnikov to abandon the Connecticut model. This comes despite advocating for that same Connecticut model in Maryland three months later. Zolnikov called out this hypocrisy:

"To say that my state doesn't deserve the right protections as four or five other states? That really didn't bode well with me."

Montana's citizen legislature, with limited staff and resources, was especially susceptible to tech lobbyists' influence. Zolnikov explained in the Senate Business, Labor, and Economic Affairs committee hearing on the bill that while national lobbyists spend years shaping

legislation, Montana lawmakers only have weeks. Zolnikov never even met the national lobbyists in-person. Instead, "technical" changes were delivered by email and phone, and often at the last minute.

Zolnikov ultimately resisted the tech lobby's most aggressive attempts at watering down the bill. Still, his experience reveals the tech lobby's playbook: overwhelm a citizen legislature with lobbyists, pressure lawmakers with last-minute edits, and rely on proxy organizations to credential the effort.

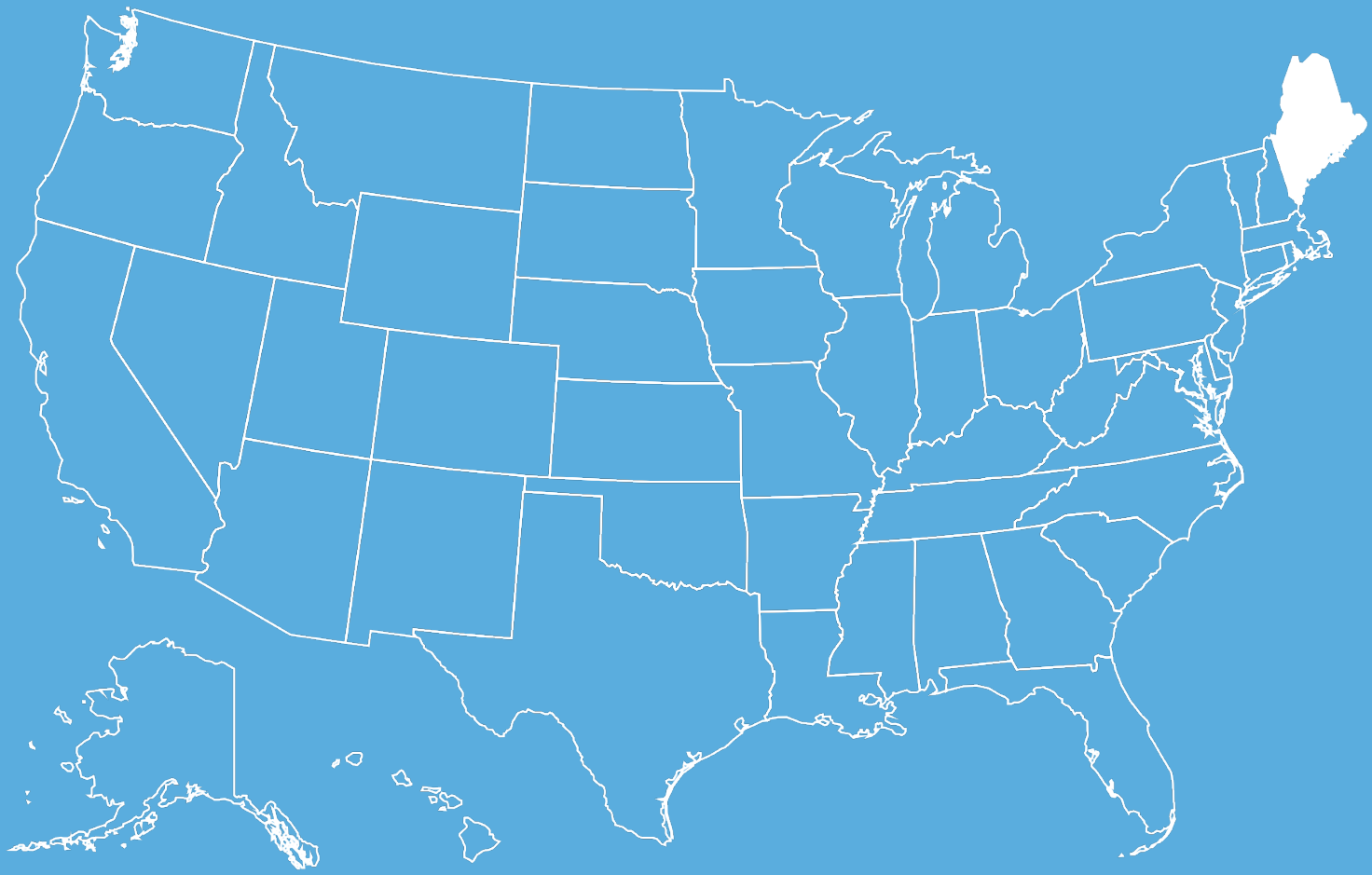
Montana Case Study Methodology

This research used lobbying disclosure data available on Montana's Principal and Lobbyist Online Reporting System which is maintained by the Commissioner of Political Practices. Lobbying reports were found under "Download Reports." To extract lobbying data from specific technology firms, the specified search terms in the footnotes were used. Because Montana's 2023 Consumer Data Privacy Act was introduced in early 2023, lobbying spending was compared across 2022 and 2023 to capture changes in lobbying activity before and after the bill's introduction.

Hearing quotes were found by watching public hearing testimony available on the Montana Public Affairs Network. Selected quotes were pulled from the Montana Senate Business, Labor, and Economic Affairs committee hearing held on February 24, 2023, accessible by this link.

3.4 The Small-Business Mirage

The tech industry's playbook includes mobilizing local chambers of commerce, retail associations, and trade groups to amplify their agenda under the guise of supporting the local economy. The Maine case study shows how this approach plays out. When faced with a strong privacy proposal that included limits on data collection and enforcement through a private right of action, the tech lobby mobilized local businesses to submit testimony and support a competing bill built around the weaker Virginia model.



Case Study 7: Maine

Co-opting the legislative process | **Flooding the zone** | **Weaponizing local businesses**

Lobbying in Maine in 2024:

Meta	Meta spent $20,400.00 in lobbying expenditures from January 2024 to April 2024, months when the company only disclosed lobbying on LD 1977 and LD 1973.
The State Privacy and Security Coalition	The State Privacy and Security Coalition spent $44,216.66 in lobbying expenditures from October 2023 to April 2024, during months when the company only disclosed lobbying on LD 1977 and LD 1973.
The Main Bankers Association	The Maine Bankers Association spent $10,700.00 in lobbying expenditures from May 2023 to April 2024, months when the company disclosed lobbying on LD 1977 and/or LD 1973.
The Maine State Chamber of Commerce	The Maine State Chamber of Commerce spent $6,180.52 on lobbying expenditures from February 2024 to April 2024, months when the company disclosed lobbying on LD 1977 and/or LD 1973.
T-Mobile	T-Mobile spent $10,250.00 on lobbying expenditures from May 2023 to April 2024, months when the company disclosed lobbying on LD 1977 and/or LD 1973.

Maine's 2024 session saw two competing data privacy bills, Rep. Maggie O'Neil's LD 1977 and Sen. Lisa Keim's LD 1973:

- ***O'Neil's LD 1977*** proposed data minimization, which limits companies to collecting only the necessary data for their services. It included expanded definitions of personal and sensitive data and a private right of action (PRA).
- ***Keim's LD 1973*** was based on the industry-friendly Virginia and Connecticut models. Meta lobbyist Andrew Hackman and Charter Communication lobbyist Kate Gore worked with Keim on the initial drafting of her bill.

The tech lobby quickly mobilized to oppose LD 1977 and support LD 1973. LD 1977 generated 256 lobbying reports, more than any other bill that session – even the state's budget. A total of 35 groups submitted written testimony on LD 1977 before the Judiciary committee's public hearing on October 17, 2023 . Among the most vocal opponents were industries like banking, retail, automotive, insurance, and healthcare.

Andrew Kingman of the State Privacy and Security Coalition submitted particularly damning testimony, arguing, "There is a clear state privacy template that now covers nearly 25% of the US population, and LD 1977 diverges so significantly from this template that it would isolate Maine's economy without providing those same protections for consumers."

Much of the written testimony echoed similar points, emphasizing that Maine should avoid creating a "patchwork" of inconsistent rules. Additionally, many called for the removal of the private right of action and the inclusion of industry exemptions to align the bill with existing laws in other states.

The following companies submitted written testimony to oppose LD 1977:

- ***Retail***: Maine State Chamber of Commerce, National Retail Federation, L.L. Bean, Association of National Advertisers, Interactive Advertising Bureau, Digital Advertising Alliance, American Association of Advertising Agencies, American Advertising Federation
- ***Healthcare***: Consumer Healthcare Products Association
- ***Automotive***: Maine Automobile Dealers Association
- ***Banking***: Kennebec Savings Bank, Maine Credit Union League, Maine Bankers Association
- ***Insurance***: The American Council of Life Insurers, State Farm Mutual Insurance Company

The following groups called for harmonization with existing industry models such as Virginia or Connecticut's data privacy legislation:

- The State Privacy and Security Coalition
- Microsoft
- The Advertising Industry
- Alliance for Automotive Innovation
- Maine State Chamber of Commerce

The following groups opposed the bill's private right of action in their testimony, arguing that the right to sue without proving harm would lead to excessive litigation:

- The State Privacy and Security Coalition
- Maine Automobile Dealers Association
- National Retail Federation
- Maine State Chamber of Commerce

The following groups called for more clarity in the bill's definitions of sensitive data, covered data, and derived data:

- The State Privacy and Security Coalition
- Microsoft
- The Advertising Industry
- Maine Automobile Dealers Association
- WEX

The following groups argued that the bill should exempt industries already covered by federal laws like GLBA (financial services), HIPAA (healthcare), and The Controlled Substances Act.

- American Council of Life Insurers
- State Farm Mutual Insurance Company
- Receivables Management Association International (RMAI)
- Maine Bankers Association
- Consumer Healthcare Products Association

While O'Neil's bill garnered support from privacy advocates, it was ultimately weakened by the tech lobby's multi-faceted strategy. The industry not only opposed LD 1977, but also promoted a more industry-friendly alternative in LD 1973. By leveraging both national lobbying groups and local business associations, the tech lobby successfully shaped the conversation in favor of the weaker bill.

By the time the session ended on April 17, neither bill had advanced, with the overwhelming volume of opposition stalling the process. This outcome mirrors a broader trend observed in other states: when stronger privacy bills gain momentum, the tech industry often avoids direct defeat by pushing a more lenient model and fostering division to block both proposals.

Maine Case Study Methodology

This research used lobbying disclosure data from the Maine Lobbyist Disclosure website, which is maintained by the Maine Ethics Commission. Data from 2023 was only available per request. 2024 lobbying spending information was found under "Advanced Search." Maine requires lobbying clients to disclose both the bills they lobbied on and the monthly lobbying expenditures. Thus, lobbying spending was aggregated across both 2023 and 2024 to capture spending on LD 1977 and LD 1973.

Written testimony was available on the Maine State Legislature website. Written testimony can be found in the Committee Testimony Display page under the 131st 2023-2024 session, selecting the Judiciary committee, and choosing the 10-17-23 date. The Senate Judiciary committee's public hearing held on October 17, 2023 is accessible by this link.

4. CONCLUSION

Across the seven state case studies, a clear pattern emerges. The technology industry has not merely influenced the direction of state privacy law; it has shaped the conditions under which these laws are conceived, drafted, and ultimately passed. In state after state, the industry succeeds not because lawmakers are indifferent to their constituents, but because they face an overwhelming imbalance of power, information, and resources.

From Washington to Maine, the industry's strategy is strikingly consistent. Lobbyists insert themselves early in the drafting process, supplying pre-written bill text under the guise of neutral "best practices." Proxy organizations appear in hearings claiming to represent consumers, small businesses, or innovative startups, while quietly funded by the largest data-collecting corporations in the world. When stronger bills gain traction, the industry "floods the zone" with weaker alternatives that sow confusion and drain limited legislative attention. And in many states — especially those with part-time sessions and skeletal staff — lawmakers end up relying on the very actors whose business models the law is supposed to regulate. The result is a wave of privacy legislation that appears protective on the surface but leaves the underlying surveillance economy almost entirely intact. The replication of the Virginia-style model across the country has created a weak, industry-designed template that now threatens to become the de facto national standard.

4.1 The Cost of Inaction

In 2025, as courts across the country grapple with lawsuits over children's safety, AI-driven manipulation, and exploitative data practices, the gap between technological power and legal protection is wider than ever. When states adopt frameworks that permit broad data collection and limited accountability, they leave the public exposed in predictable and avoidable ways.

For children and teenagers, the risks are especially acute. Recent litigation has revealed how platforms use extensive data on mood, behavior, and attention patterns to shape what young people see and how long they stay online. Without strong limits on data collection, companies can continue profiling teens across apps and devices, fueling algorithmic recommendation systems that amplify harmful content and undermine mental health. Weak state laws leave these practices largely untouched.

For national security, the stakes have sharpened. Investigations and federal actions over the past year have highlighted how sensitive location data, biometric identifiers, and detailed personal histories continue to be collected by data brokers with minimal oversight. Foreign adversaries no longer need to breach secure government or corporate systems when they can simply purchase vast troves of sensitive data on Americans through the open commercial market. This data can be exploited for intelligence gathering, surveillance, blackmail, targeting of military personnel and public officials, and large-scale influence operations. Weak state privacy laws leave these channels wide open, effectively subsidizing foreign intelligence access to the daily movements, vulnerabilities, and relationships of the U.S. population.

But the deepest damage is to the integrity of the information ecosystem itself. The rapid

integration of AI into search, social platforms, advertising, and news distribution has given companies unprecedented influence over what information reaches the public and how it is framed, ranked, or omitted. These systems are fed by immense behavioral datasets that individuals never meaningfully consented to share. With weak privacy laws in place, companies can continue refining AI models on personal data that shapes everything from targeted political messaging to the very structure of online discourse.

This is not just a privacy problem; it is a democratic one. A society cannot make collective decisions when its information environment is privately engineered, personalized, and opaque. In the absence of strong protections, a handful of companies control the levers of attention and access to information, quietly determining which voices are amplified, which narratives spread, and which communities see which versions of reality.

Inaction now means allowing these systems to harden by default, giving unaccountable actors continued power to shape civic life from behind the scenes. The cost is not only the ongoing exposure of individuals: it is the erosion of the shared public sphere on which American democracy depends.

4.2 The Opportunity Ahead

Yet the trajectory is not fixed. These case studies also reveal moments of resistance, proof that industry dominance is not inevitable. Transparency can shift legislative dynamics. Coordinated advocacy can reshape political incentives. And lawmakers can reject industry scripts when they understand what is at stake.

Maine's lawmakers saw through the tech lobby's small-business mirage. Maryland passed a data-minimization privacy law in 2024, becoming the only state outside California to adopt a rights-protective framework rooted in limiting data collection at the source. And in 2025, not a single industry-written privacy bill passed in any state, a clear signal that legislators are beginning to recognize and push back against the playbook.

The country is now at an inflection point. In the 2026 legislative cycle, dozens of states will consider privacy bills. Federal lawmakers continue to debate national legislation, including a Republican Privacy Working Group in the House Committee on Energy & Commerce. The rules that will govern the next decade of the data economy are being written now. Whether the U.S. builds a rights-based privacy framework or cements a surveillance-driven one will depend on who shapes the next wave of policymaking: the public or industry.

Rebalancing the policy landscape will require more than stronger bill text. It will require changing who gets to shape that text in the first place. Different actors hold different kinds of leverage: federal policymakers control the national baseline; state legislators control the standards that spread; attorneys general control enforcement; civil society and academics fill the expert vacuum; journalists shape public understanding; small businesses can refuse to be used as industry props; and residents ultimately set the democratic pressure that legislators respond to.
For that reason, the path forward must be multi-layered. The following recommendations outline specific, actionable steps each group can take to counter the influence documented in this report and steer the country toward meaningful privacy protections.

4.3 Recommendations

Actions for Federal Policymakers

Congress and federal agencies have the power to establish a strong national baseline without cementing the industry's weakest state standards.

1. ***Look beyond weak state standards.*** Do not treat the Virginia model or other industry-influenced state laws as a template for federal legislation. These frameworks were not the product of democratic consensus or robust policy analysis; they were engineered under conditions of industry dominance and legislative resource scarcity.
2. ***Pass a strong, comprehensive federal privacy law.*** Adopt legislation that includes data minimization, strict limits on sensitive data, enforceable consumer rights, and algorithmic accountability. The federal standard should act as a floor, not a ceiling, preserving states' ability to exceed it in traditional areas of state leadership such as education, consumer protection, and worker protections.
3. ***Ensure meaningful accountability.*** Grant the FTC expanded enforcement authority, require annual rulemaking on emerging technologies, and include a private right of action so individuals can seek redress when harmed. Provide stable federal funding for enforcement to avoid regulatory capture and ensure durable, long-term oversight.
4. ***Mandate transparency in data and AI practices.*** Require companies, data brokers, and platforms to disclose: how personal data is used to train or optimize AI systems; how targeting and recommendation algorithms operate; and what categories of sensitive data they collect, purchase, or infer. This includes mandatory public reporting on high-risk AI systems, safety evaluations, and data sourcing.

Actions for State Policymakers

States remain the front line of privacy law. To counter the industry's structural advantages, states must strengthen both substance and process.

1. ***Adopt strong guardrails—not industry models.*** Ensure that any privacy bill includes: data minimization and purpose limitation; strong protections for sensitive data, including location, biometric, and health data; no broad "business purposes" exemptions; enforcement by both the Attorney General and a private right of action. These protections distinguish strong privacy laws from industry-backed templates.
2. ***Increase transparency in the legislative process.*** Ask for disclosure when lobbyists or trade associations contribute bill text, amendments, or "technical fixes." Committee reports should identify model language and the source of any external redlines. States should also strengthen gift and conflict-of-interest rules for outside policy advisors.
3. ***Build in-house expertise.*** Expand capacity within nonpartisan legislative counsel offices. Establish technology-policy fellowship programs funded by universities, philanthropic organizations, or state appropriations (not industry). Train staff to research lobbying networks and understand the interests behind testimony, model bills, and "neutral experts."
4. ***Strengthen enforcement.*** Fund specialized Attorney General privacy units, including technical investigators and litigators familiar with digital forensics, data broker ecosystems, and AI systems. Enable multistate coalitions to coordinate enforcement actions against data brokers and dominant platforms.
5. ***Improve coordination across states.*** Leverage independent public-interest organizations—such as policy experts from EPIC and Consumer Reports—to share rights-protective

model legislation, track amendments, identify industry-backed provisions, and maintain a shared database of lobbyist positions across states. Separately, scrutinize and disclose the funding of interstate coordinating bodies and policy associations to ensure their agendas are not shaped by major technology companies.

Actions for Civil Society, Advocacy Organizations, Academics & Researchers

Public-interest actors play a crucial role in counterbalancing industry power and filling the expertise gap inside statehouses.

1. ***Align around a shared set of "non-negotiables."*** Develop and maintain a unified, rights-protective model bill (such as EPIC's State Data Privacy Act, that strengthens the Connecticut model) with data minimization, PRA, strong agency enforcement, and modern sensitive data protections. Consistency across states increases political clarity and momentum.
2. ***Fill the expert vacuum.*** Expand capacity to provide technical briefings, publish accessible bill analyses, and track amendments in real time. Coordinate with the few organizations that do work on the ground across many states, such as EPIC and Consumer Reports, to ensure lawmakers hear aligned, evidence-based guidance rather than fragmented advocacy.
3. ***Expose lobbying networks and proxy organizations.*** Map relationships between tech companies, their trade associations, local chambers, and purportedly "consumer" or "small business" coalitions. Publish reports and testimony that clearly identify funding sources and influence networks so committee hearings are grounded in transparency.
4. ***Connect privacy harms to broader public concerns.*** Help lawmakers and communities understand how unchecked data collection affects areas they already care about such as youth mental health, national security risks, reproductive care privacy, AI-driven misinformation, and worker monitoring. Provide case studies and local examples.
5. ***Support grassroots participation.*** Offer advocacy toolkits, training sessions, and step-by-step guides for submitting testimony, calling legislators, and tracking amendments. Partner with bipartisan community groups — parent associations, veteran groups, health coalitions, local libraries, etc. — to broaden the coalition and embed privacy in existing civic networks.

Actions for Journalists

Statehouse reporters and investigative journalists shape how the public understands privacy laws—and whether lawmakers are held accountable.

1. ***Follow the origins of bill text.*** Ask legislators who drafted the bill and who provided the amendments. Compare language with known industry templates. Treat authorship as a central part of the story, not a procedural detail.
2. ***Investigate lobbying networks.*** Use lobbying disclosures, funder statements, testimony archives, and corporate filings to trace the influence of trade associations, proxy groups, and local chambers acting as stand-ins for Big Tech.
3. ***Reframe coverage of privacy debates.*** Move beyond consumer-choice tropes. Highlight structural power: who benefits, who bears the risks, and what types of data practices the bill actually allows. Emphasize not what the bill claims to do, but what it permits to continue.
4. ***Spotlight the stakes for kids, national security, and democracy.*** Explore how data collection fuels harmful youth-content algorithms, creates national-security vulnerabilities through data brokers, and shapes information flows via AI-driven content

ranking. Connect privacy to the integrity of the information ecosystem.

5. ***Elevate state-level consequences.*** Illustrate how small or rural states can set precedents adopted nationwide. Explain how industry pushes weak templates from one state to the next, and how a single strong or weak bill can influence federal debates.

Actions for Small Businesses & Local Business Associations

Small businesses are often used as political cover for Big Tech, despite fundamentally different interests.

1. ***Develop independent views on privacy.*** Use reputable resources — such as the Federal Trade Commission's business education guides, Consumer Reports, and state consumer protection offices — to form your own judgment on whether the current data economy helps or harms your business.
2. ***Demand transparency from state trade associations.*** Ask your state chamber of commerce and local business groups who writes their privacy policy positions, who funds their advocacy, and consider whether those positions reflect the interests of multinational platforms rather than local businesses.
3. ***Resist being used as political cover.*** Decline to sign letters or testimony that misrepresent small-business needs. Consider testifying independently about why strong privacy protections promote fair competition and a level playing field.

Actions for Concerned Residents & Grassroots Organizers

Public engagement remains one of the strongest forces against industry capture. Residents can shift political incentives when they know what to look for.

1. ***Watch for red flags in any state privacy bill,*** like no private right of action; minimal or no data minimization; broad exemptions (e.g., "business purposes" or "derived data"); and industry groups testifying as "neutral" experts. These are common signs of an industry-driven bill.
2. ***Engage early in the process.*** Submit testimony, attend hearings, call legislators, and ask for explanations of bill language. Legislators pay attention to active constituents, especially in states where few residents typically engage.
3. ***Ask direct, high-impact questions.*** Examples: "Who wrote this bill?" "Does this law limit how much data companies can collect?" "Why is this weaker than the laws in California or Maryland?" "Does this bill allow data brokers to keep selling my location data?"
4. ***Build cross-issue coalitions.*** Partner with parents, teachers, youth organizations, librarians, veterans groups, health advocates, and civic associations. Privacy harms cross traditional issue boundaries.
5. ***Demand that lawmakers reject industry-written models.*** Public pressure — especially in small, part-time legislatures — can block weak bills and strengthen good ones. Organize call-in days, coordinate testimony, and ask lawmakers to commit publicly to independent lawmaking rather than outsourcing drafting to industry lobbyists.

Taken together, these actions point to a simple conclusion: privacy is no longer a niche consumer issue, but a prerequisite for democratic self-government in the digital age. Statehouses can be laboratories of rights or laboratories of industry capture. Which path the country takes will depend on whether lawmakers, advocates, journalists, small businesses, and residents insist that the rules of the data economy be written in public, for the public.