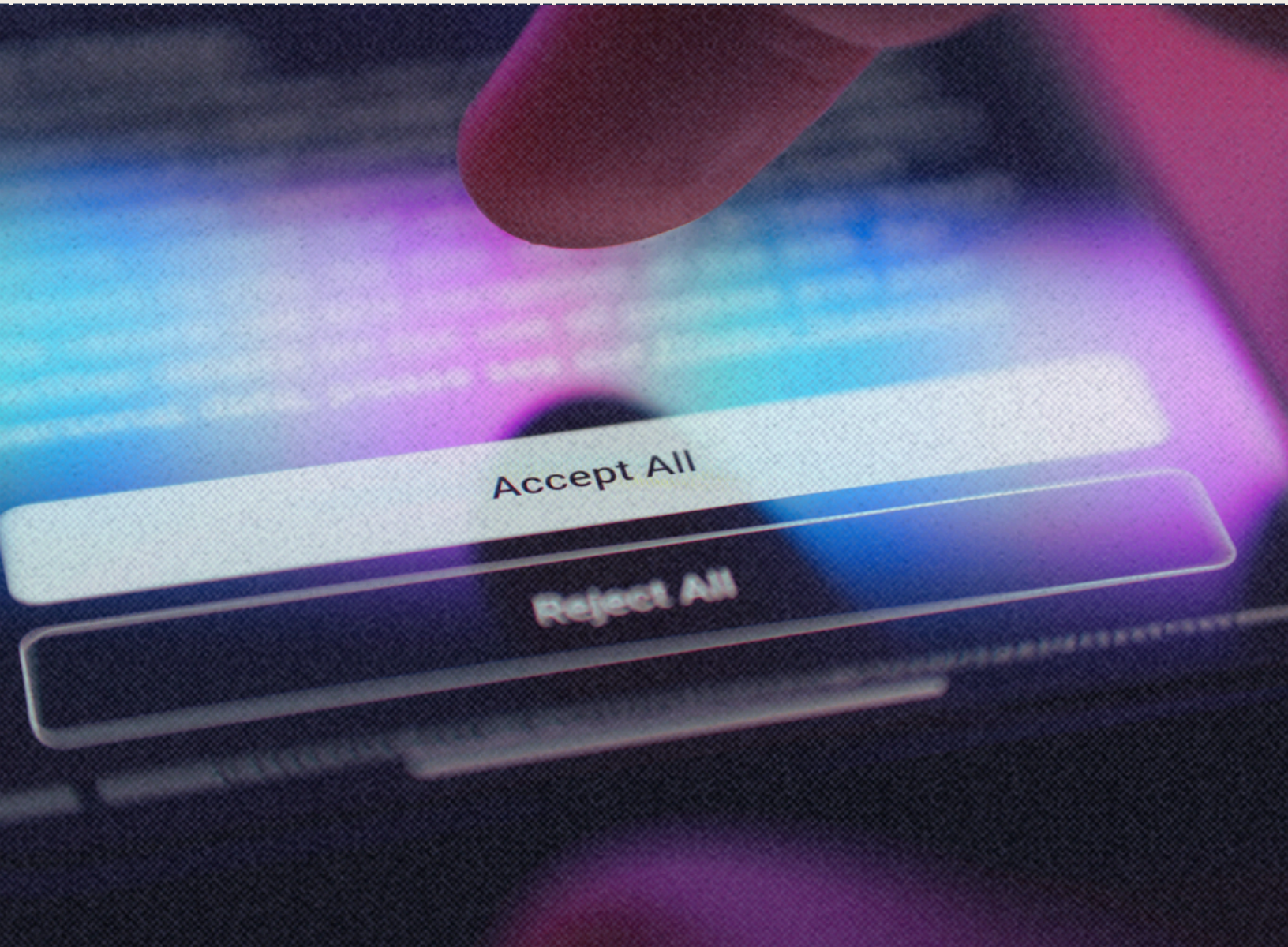
REPORT | APRIL 2026

The Inescapable Link: How Data Policy Still Dominates Tech Policy Debates

By Tirzah Duren and Logan Kolas



Executive Summary

For more than two decades, Congress has tried and failed to establish a national data privacy standard. States have responded by filling in the gaps with a patchwork of rules and data regulations, each with their own unique reporting obligations and compliance requirements. As state lawmakers continue to introduce and amend their now entrenched data privacy regimes, compliance costs are compounding as federal policymakers have pivoted to other pressing policy matters: kids online safety, competition in technology markets, and artificial intelligence regulation. Although many federal policymakers have seemingly moved on from the established privacy debates, data regulation remains a "missing link" to ongoing technology policy conversations that threaten to undermine consumer freedom in emergent technology domains. Unfortunately, the reality remains that topical technology debates are recycling long-held policy disagreements on data regulation. To address those issues, Congress must revisit data privacy and agree to a light-touch and preemptive standard.

Introduction

Since the European Union implemented the General Data Protection Regulation (GDPR) in 2018, many privacy experts have lamented that the United States is falling behind in privacy protection. These critiques overlook extensive sector-specific rules, including privacy protections for health, education, financial data, and the Federal Trade Commission's (FTC) authority over dishonest privacy disclosures through its Section 5 deceptive practices authority. Still, the current data privacy regime is inconsistent, filled with gaps, and subject to the discretion of the bureaucrats who enforce it.

A comprehensive federal data privacy standard would be justified if only to pre-empt a growing patchwork of independent state compliance regimes that threaten innovation—but the benefits could be far greater. A properly designed federal data privacy framework would inform subsequent regulations, provide certainty as a foundation for innovation, fill a market need for clarity in legal proceedings, place needed guardrails on bureaucratic power expansions, and even provide a roadmap for international data flow governance.

Despite its centrality, federal policymakers have repeatedly failed to enact a comprehensive privacy framework. That inaction, however, has not rendered data privacy peripheral. Instead, privacy concerns increasingly animate a wide range of regulatory and policy debates—including artificial intelligence governance, the scope of FTC enforcement authority, antitrust remedies in data-driven markets, industrial and social policy, and national security.

The breadth of these issue areas underscores a critical reality: data privacy is a foundational substrate underlying contemporary technological governance. Any attempt to regulate emerging or current technologies without addressing privacy directly risks incoherence, overreach, and regulatory fragmentation.

Tennessee as a Sample Data Privacy Framework

Tennessee provides a worthy template for other states—and for federal policymakers—in drafting appropriate data privacy standards. Governor Bill Lee signed the Tennessee Information Protection Act (TIPA) in 2023 before it took effect on July 1, 2025. The law applies to businesses operating in Tennessee with an annual revenue of at least $25 million and that meet a minimum threshold for users and revenue shares. The law includes "cure" periods where companies can rectify violations before being subject to legal action, which helps to stay overeager state enforcers who have looked to expand other state data privacy laws beyond their intent. It also includes a novel approach to enforcement by providing companies an "affirmative defense" in court if they comply with data privacy best-practices from the National Institute for Standards and Technology (NIST). Similar to many other state data privacy regimes, Tennessee also sets forward certain "rights" for consumers and obligations on companies.

CONSUMER RIGHTS

- Right to access: Confirm whether a controller is processing their data and view the information processed.
- Right to correction: Request correction of inaccurate personal information.
- Right to deletion: Request deletion of personal information (with reasonable exceptions for aggregated or de-identified data).
- Right to portability: Obtain a copy of their personal data in a portable format.
- Right to opt-out: Opt-out of the sale of personal information, targeted advertising, and profiling based on personal data.

BUSINESS OBLIGATIONS

- Purpose limitation: Limit data collection to purposes identified in privacy disclosures and avoid processing that is incompatible with those purposes unless consent is obtained.
- Security measures: Implement reasonable safeguards against unauthorized access and use.
- Privacy notice: Provide clear privacy notices that describe consumer rights and how to exercise them.
- Controller-Processor Contracts: Written contracts must govern relationships between data controllers and processors, including confidentiality duties and compliance mechanisms.

Like all state data privacy models, Tennessee is imperfect in its approach to data privacy—impact assessments, for example, threaten to impose all kind of open-ended paperwork requirements. But if the federal government were to take a page from the Tennessee privacy framework, and add necessary improvements, it would establish a worthwhile standard among state approaches and help inform current regulatory conversations including child protection, AI, antitrust, national security, and industrial policy.

Child Protections Should Not Be Built from Scratch

Protecting children online has emerged as a rare point of bipartisan consensus in U.S. technology policy. With near-equal support from Republicans and Democrats, the Kids Online Safety Act (KOSA) represents one of the most prominent federal efforts to recalibrate how digital platforms interact with younger users.[1] Similarly, the Children and Teens' Online Privacy Protection Act 2.0 (COPPA 2.0), which recently passed the Senate by unanimous consent, seeks to update earlier child-focused privacy laws by extending statutory protections to users under the age of 17, rather than the current threshold of 13.[2]

Although these proposals are framed primarily as child safety measures, both rely heavily on broad restrictions on the collection, processing, and use of personal data. In doing so, they bring child-specific safety concerns into wider debates over data practices—such as targeted advertising and algorithmic personalization—that affect users of all ages. This approach risks conflating distinct policy objectives. A comprehensive data privacy regime would provide a more stable foundation for additional child-specific protections where warranted, while simultaneously addressing broader consumer concerns about data use and governance. Addressing broader data concerns through limited child focused legislation leaves actual data concerns unresolved.

Public sentiment supports the need for a foundational approach. A survey of 1,500 users across the United States and Canada found that 62 percent of respondents feel uncomfortable with online tracking.[3] Addressing these concerns requires a transparent discussion of trade-offs, consent mechanisms, and opt-out rights applicable across the digital ecosystem—not narrowly tailored prohibitions aimed at specific age cohorts. Yet current federal proposals remain largely piecemeal, targeting discrete populations while layering expansive regulatory obligations that have proven difficult to reconcile across political and institutional lines.

TIPA offers a more coherent alternative by embedding child protections within a broader, generally applicable privacy framework, not the other way around. Under TIPA, the personal data of children under the age of 13 is automatically classified as sensitive, triggering heightened safeguards, including affirmative consent requirements and the ability for a verified parent to exercise rights on a child's behalf. At the same time, the framework preserves flexibility by permitting age-appropriate personalization and data use—subject to broad transparency and security obligations—rather than imposing categorical bans.

[1] S. 1409 — Kids Online Safety Act, Introduced May 2, 2023, https://www.congress.gov/bill/118th-congress/senate-bill/1409.
[2] S. 1418 — Children and Teens' Oline Privacy Protection Act, Introduced May 3. 2023, https://www.congress.gov/bill/118th-congress/senate-bill/1418/text; and Anna Merod, "Kids Internet and Digital Safety Act Advances to Full House Vote," K-12 Dive, March 9, 2026, https://www.k12dive.com/news/kids-online-safety-act-moves-to-a-vote-on-the-full-house-floor/814216/.
[3] GumGum Team, "Consumers Say No to Data Tracking—Here's How Advertisers Should Respond," GumGum, March 19, 2025, https://gumgum.com/blog/consumers-say-no-to-data-tracking.

This calibrated approach stands in contrast to federal proposals such as KOSA and COPPA 2.0, which either restricts personalized recommendations or prohibits targeted advertising to minors altogether. Such prohibitions risk eliminating data that may be necessary to design safer, more tailored online environments for children, while failing to address underlying concerns about data governance across the broader population. By focusing on consent, sensitivity, and accountability rather than outright bans, the Tennessee framework mitigates these risks better than most.

TIPA also avoids several definitional and structural challenges that complicate federal child safety legislation. For example, KOSA's reliance on vague concepts such as "compulsive usage" creates significant interpretive uncertainty, potentially encompassing benign or developmentally normal online behavior, while simultaneously applying only to digital platforms rather than comparable offline activities. Embedding child protections within a general privacy framework reduces reliance on such indeterminate standards and limits the scope for discretionary or uneven enforcement.

Ultimately, Tennessee creates a coherent and universal data privacy regime that protects children online without introducing conceptual ambiguity and regulatory overreach present in KOSA and COPPA 2.0. By establishing baseline guardrails applicable to all users, while layering enhanced protections for minors, the Tennessee model demonstrates how child safety objectives can be achieved without fragmenting privacy policy or undermining broader consensus on data governance.

Data Privacy Is a Missing Foundation for AI Development

Artificial intelligence depends on vast volumes of data to identify patterns, refine models, and generate usable outputs. Without reliable access to high-quality data, AI systems cannot function. That reality makes data governance not a peripheral issue, but the bedrock of every meaningful policy discussion surrounding AI.

Notable lawmakers from Senator Maria Cantwell and Senator John Hickenlooper have emphasized this reality through statements on the need for a privacy bill to underpin future AI regulations.[4] Clear, comprehensive, and predictable data privacy rules are essential to providing regulatory certainty for emerging technologies. A national framework—light-touch in design yet strong enough to safeguard individual rights—would offer the stable foundation developers, businesses, and consumers need to innovate responsibly.

[4] Gopal Ratnam, "Data Privacy Law Seen as Needed Precursor to AI Regulation," RollCall, September 26, 2023, https://rollcall.com/2023/09/26/data-privacy-law-seen-as-needed-precursor-to-ai-regulation/.

From the consumer perspective, growing unease around data use is compounded by persistent confusion. Americans routinely express support for data privacy protections, yet few fully grasp what their consent entails.[5] In one study, 98 percent of participants failed to notice a clause in a fake consent form that granted the researcher naming rights to their firstborn child.[6] Research from the University of Pennsylvania similarly found that most consumers do not understand how their data is used within the broader digital ecosystem.[7] This confusion is likely to deepen as AI introduces additional layers of opacity and complexity.

Debates over the types of data AI systems can—or should—use often pit competing incentives against one another—everything from intellectual property safeguards to platforms pursuing revenue through licensing agreements and social norms.[8] As AI reshapes norms on social media specifically and on the internet broadly, the concept of "contextual integrity" offers a useful framework for AI privacy. Contextual integrity is the idea that privacy does not function as an absolute right to secrecy or to exclude information from others in all cases, but instead that privacy flows according to context-specific social norms of who shares what, with whom, and on what terms. When AI violates the norms consumers have accepted over time—or generates new use cases entirely—it invites backlash and causes general social unease.[9]

Although social media content likely qualifies as "publicly available" information under existing laws, consumers can experience social discomfort when their information is repurposed or augmented by AI, specifically because new social norms are still evolving. For this reason, it would be prudent for policymakers to pursue flexible governance approaches on privacy that can evolve with changing social norms.

Tennessee's privacy approach navigates this divide better than most. Its light-touch and adaptable framework does not explicitly regulate artificial intelligence systems, but it still contributes meaningfully to the AI policy debate, nonetheless. Its affirmative defense for compliance with NIST best-practices on privacy encourages companies to align internal business practices with a system of privacy norms that have evolved normatively through a system of trial-and-error over decades. Since privacy guidelines are updated frequently, business practices can evolve alongside shifting privacy structures. And like nearly all state data privacy laws, Tennessee excludes publicly available data from its privacy framework. It therefore delineates the boundary between data protection and other unresolved issues, such as fair use and intellectual property. This separation channels those debates into more appropriate policy venues, rather than further complicating an already fragmented data privacy landscape.

---

[5] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "4. Americans' Attitudes and Experiences with Privacy Policies and Laws," Pew Research Center, November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.
[6] Brett Cruz and Gene Petrino, "Americans Get an F on Digital Privacy Knowledge," Security, April 1, 2025, https://www.security.org/digital-security/american-digital-privacy-knowledge/.
[7] Hailey Reissman, "Americans Don't Understand What Companies Can Do With Their Personal Data—and That's a Problem" University of Pennsylvania, February 7, 2023, https://www.asc.upenn.edu/news-events/news/americans-dont-understand-what-companies-can-do-their-personal-data-and-thats-problem.
[8] Ryan McGrady, "AI Companies Threaten Independent Social Media Research," Tech Policy Press, January 20, 2025, https://www.techpolicy.press/ai-companies-threaten-independent-social-media-research/.
[9] Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119 (2004), https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/.

AI also highlights some of the current limitations of data privacy rules. Like most state data privacy regimes, Tennessee includes a right for consumers to delete information about them, subject to carveouts for aggregated, de-identified, and pseudonymous consumer data. These exemptions already provide meaningful relief in AI applications, where exact machine unlearning is difficult because data is embedded in model weights and parameters. They are especially valuable in the AI context because data deletion obligations remain impractical due to the limits of model "unlearning" technology. Innovators have made great strides in "deletion" technology, but data "deletion" is merely data "suppression." For that reason, model retraining is the "gold standard"—but the process is time-consuming, repetitive, expensive, and favors large companies with resources over fledgling startups with thin profit margins.[10]

A model federal bill would therefore exclude or exempt anonymized and truly pseudonymous data from deletion rights in the AI context. Through these limited changes and clarifications, the Tennessee privacy approach would inform AI policy by prioritizing worthwhile transparency requirements regarding data collection, use, and sale—a significant step toward building consumer trust. Enhanced disclosure enables greater public understanding of general data practices and more specifically how AI systems obtain and deploy data, addressing concerns that cannot be resolved through access-and-delete mandates alone.

The Tennessee framework not only strengthens consumer protections on existing digital platforms but also establishes durable, forward-looking norms for emerging technologies such as AI. By setting clear expectations, policymakers can support innovation while safeguarding consumer rights in an increasingly data-driven environment.

The FTC's Role: Filling the Gap, Risking Overreach

The FTC has emerged as Uncle Sam's chief privacy enforcer. It relies primarily on notice-and-consent and its Section 5 authority under the FTC Act—which allows the agency to police data privacy violations as "deceptive trade practices."[11] This protection and enforcement regime functions by enforcing publicly disclosed commitments. When companies fall short of their promises, the FTC treats those violations as deceptive activity. At its core, these powers promote minimally invasive consumer protection based on the principle of informed consumer consent. However, critics have continually pointed out that data disclosures are difficult to understand, and that want of understanding undermines consumer consent.[12]

[10] A. Feder Cooper et al., Machine Unlearning Doesn't Do What You Think: Lessons for Generative AI Policy and Research, arXiv:2412.06966v2 (Last revised October 31, 2025), https://arxiv.org/abs/2412.06966.
[11] Steve Pociask and Isaac Schick, "Section 5 and Proper FTC Enforcement," American Consumer Institute, June 22, 2023, https://www.theamericanconsumer.org/2023/06/section-5-and-proper-ftc-enforcement/.
[12] Totyana Norman-Webler, "How Both Washington and the FTC Miss the mark on "Notice and Consent," Cleveland Metro Bar Association, March 20, 2024, https://www.clemetrobar.org/?pg=CMBABlog&blAction=showEntry&blogEntry=104787.

To address these shortcomings, some experts have proposed that consent notices be written without industry jargon and at a reading level reflective of the general adult population. Many states do this in some form already. For example, as a part of Tennessee's data privacy law, companies are required to provide a "reasonably accessible, clear, and meaningful privacy notice." Still, clarifying federal disclosure guidelines could help states ensure that full transparency is reached in ways that don't risk FTC intervention.

There is the risk that the FTC is not content to restrict its actions to this clear area of Congressionally authorized authority.[13] In 2022, the agency issued an advanced notice of proposed rulemaking on commercial surveillance and data security, signaling an intent to expand its regulatory reach.[14] No formal trade regulation rules have materialized and with new leadership the agency appears unlikely to continue these efforts at this time. But the move laid bare the risks of unchecked agency powers and heightened fears of government overreach, particularly given perceptions of politicization within the agency.[15]

Rather than creating a vacuum for states and agencies to fill in piecemeal, Congress can provide a framework which includes disclosure requirements and a narrowly tailored scope for agency enforcement that sets clear guardrails on agency powers. Legislating is the job of Congress, not unelected bureaucrats.

Data Contradictions at the Heart of the Google Antitrust Cases

The FTC and Department of Justice (DOJ) are the agencies tasked with federally enforcing antitrust and protecting competition in the United States. As shown by recent cases involving Google, the implications of a federal data privacy regime extend beyond congressional regulations to the regulation of competition itself. Establishing a federally comprehensive data privacy law would establish standard protection, influence data use in competition, and create guidelines for proposed remedies, rather than putting judges in the uncomfortable position of effectively legislating data policy from the bench.

In August 2024, U.S. District Judge Amit Mehta ruled that Google's use of "default status" agreements allowed it to illegally maintain a monopoly in online search in violation of Section 2 of the Sherman Antitrust Act. As the judge sees it, default status contributed to Google's size and led to a flywheel effect: greater access to consumers created greater access to data and created an advantage against its competitors, thus allowing the company to create better algorithms and maintain better product services at scale.[16] That led to more and better data access, creating a self-perpetuating cycle.

[13] Woodrow Hartzog and Daniel J. Solove, The Scope and Potential of FTC Data Protection, 83 National Law Center of the George Washington University, 22230 (2015), https://scholarship.law.bu.edu/faculty_scholarship/3041/.
[14] Federal Trade Commission, "Commercial Surveillance and Data Security Rulemaking," August 11, 2022, https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.
[15] Tirzah Duren, "Bad Antitrust Is a Barrier to Data Privacy," Free the People, June 11, 2024, https://www.theamericanconsumer.org/2024/06/bad-antitrust-is-a-barrier-to-data-privacy/.
[16] Abigail Slater, "Why 'Big Data' Is a Big Deal," The Regulatory Review, November 6, 2023, https://www.theregreview.org/2023/11/06/slater-why-big-data-is-a-big-deal/.

The DOJ alleged that Google's anticompetitive conduct harmed consumers by causing deteriorated search quality along "dimensions such as privacy, data protection, and use of consumer data."[17] As a part of the remedy process, the DOJ argued that Google should be forced to share its data with competitors to improve their algorithms and compete at scale.[18]

In a separate April 2025 case, Judge Leonie Brinkema ruled that Google violated Section 1 and 2 of the Sherman Antitrust Act by holding a monopoly in the ad-tech market.[19] To remedy those violations, the DOJ has proposed four "data and transparency" measures, which the DOJ believes will rectify the "data and scale advantages" that allowed Google to derive benefits from its anticompetitive conduct and scale advantages.[20]

These cases emphasize the use of data as a competitive asset; however, the remedies phases focus on the sharing of this data without much consideration over the originating consumers. In the official remedy for the Google search case, Judge Mehta required that Google share some data with competitors to help improve competing search.[21]

Data sharing may be an appropriate remedy from a competition angle, but it only adds to the lack of control that consumers already feel. According to 2023 Pew Research polling, about 73 percent of respondents reported feeling a lack of control over what companies do with their data while 67 percent reported a lack of knowledge over its use.[22]

A comprehensive data privacy regime likely would not have prevented the antitrust cases or the verdicts, but it would inform behavior by providing a clear line in the sand. As shown in the Google case, a judge was left to determine data sharing parameters, which are outside their expertise.

Clarifying the ways companies can collect, process, use, and transfer data would establish protection and reduce confusion.

Beyond Google, ongoing cases, such as the FTC's case against Amazon, which accuses the online platform of unfairly using data to compete against third-party sellers, would be better informed by comprehensive data protection. Lack of guardrails introduces a reliance on subjective enforcement as neither the company nor agency has a clear outline of legislative protection to inform behavior or cases.

[17] Caitlin F. Saladrigas, Rachel Marmor, David C. Kully, and Ryan Kocse, "Google Search: Data Sharing as a Risk or Remedy?," Holland & Knight, April 15, 2025, https://www.hklaw.com/en/insights/publications/2025/04/google-search-data-sharing-as-a-risk-or-remedy#:~:text=The%20core%20focus%20of%20the,Google%20algorithms%20and%20deliver%20better.
[18] David Spector, "FTC Backs DOJ Plan to Force Google to Share Search Data with Competitors in Landmark Antitrust Case," May 13, 2025, https://www.foxbusiness.com/media/ftc-backs-doj-plan-force-google-share-search-data-competitors-landmark-antitrust-case.
[19] Ilyse Liffreing, "Google is an Ad Tech Monopolist: U.S. Judge Rules and Industry Responds," The Current, April 17, 2025, https://www.thecurrent.com/data-privacy-google-ad-tech-monopolist-us-judge-rules-industry.
[20] Joseph V. Coniglio, "The DOJ's Problematic Remedies Proposal in the Google Ad Tech Case," Information Technology & Innovation Foundation, May 12, 2025, https://itif.org/publications/2025/05/12/the-dojs-problematic-remedies-proposal-google-ad-tech-case/.
[21] United States of America et al v. Google LLC, No. 1:20-cv-03010 (APM), Document 1436 (D.D.C. Sept. 2, 2025) (Redacted Memorandum Opinion), https://law.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2020cv03010/223205/1436/.
[22] Colleen McClain, Mi8chelle Faverio, Monica Anderson, and Eugene Park, "How Americans View Data Privacy," Pew Research Center, October 18, 2023, https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/#:~:text=The%20public%20increasingly%20says%20they,and%20the%20government%20(79%25).

Data Transfer Requirements Were Central to the U.S. TikTok Debate

Data privacy discussions revolve around private industry access and use of personal data—but governments are equally significant offenders at both the national and international levels. In fact, the issue of data transfers between nations is central to the U.S. national security debate surrounding TikTok. In April 2024, President Biden signed into law the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA), which specifically targeted TikTok and its parent company, ByteDance, over concerns that Chinese laws could compel the company to share U.S. user data with the Chinese government.[23] Given China's distinction as an adversarial nation under the law, PAFACA forced ByteDance to divest from TikTok or face a ban in the United States. After years of debate and negotiations, TikTok has agreed to a divestment agreement which focuses on domestic ownership and oversight, finalizing its sale in late January of 2026.[24]

While the merits of the overarching data concerns remain classified, initial proposals to ban TikTok would have done little to prevent foreign access to U.S. data, as other avenues for data acquisition remain unaddressed. As researchers at the Atlantic Council's Digital Forensic Research lab explained, "the data that TikTok can provide on Americans pales in comparison to what the Chinese government has accessed through both its illegal hacking activities and what is available legally on the open market through US-based third-party data brokers."[25]

The lack of a comprehensive data privacy framework therefore complicates efforts to address the alleged risks associated with TikTok and similar entities. In the absence of clear, overarching guidelines for data handling and security, legislative solutions are inevitably piecemeal, focusing narrowly on individual companies rather than establishing uniform standards applicable across the tech sector. A more comprehensive approach would provide neutral, enforceable tools to regulate any company—domestic or foreign—found to be violating data privacy or security requirements.

[23] H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act, Introduced March 5, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7521/text.

[24] Max Zahn and Selina Wang, "What the Deal Between TikTok and US Investors Means for Users," ABC News, December 19, 2025, https://abcnews.go.com/Business/deal-tiktok-us-investors-means-users/story?id=128551312#:~:text=Here's%20what%20to%20know%20about,executive%20order%20signed%20by%20Trump; David McCabe and Emmett Lindner, "TikTok Strikes Deal for New U.S. Entity, Ending Long Legal Saga," New York Times, January 22, 2026, updated January 23, 2026, https://www.nytimes.com/2026/01/22/technology/tiktok-deal-oracle-bytedance-china-us.html; and Great Cross, "Will TikTok Be Banned on June 19? Trump Says He'll Extend the Deadline Yet Again, If Needed," USA Today, May 6, 2025, https://www.usatoday.com/story/tech/2025/05/06/trump-extend-tiktok-ban-deadline/83480432007/.

[25] Atlantic Council Experts, "Your Expert Guide to the Debate Over Banning TikTok, Atlantic Council, January 9, 2025, https://www.atlanticcouncil.org/blogs/new-atlanticist/your-expert-guide-to-the-debate-over-banning-tiktok/.

Looming Data Privacy Threats in Wake of Congressional Dysfunction

Federal approaches to online digital regulation often treat data privacy as a secondary consideration in addressing other policy objectives. Look no further than the American Innovation and Online Choice Act (AICOA), which primarily sought to curb perceived platform dominance with bans or limitations on self-preferencing, product discrimination, and interoperability.[26]

As Congress seeks new avenues of technology regulation in 2026, a new iteration of AICOA is rumored to be in the works.[27] Time will tell if the new version is better than the old one, but in the most recent iteration of AICOA, normal business activity was plagued by all manner of regulations and restrictions on the use, access, and sharing of consumer data—which itself provides immense consumer benefit. Chief among its data provisions were restrictions on the use of data generated by third-party businesses and prohibitions on platforms limiting third-party access to this data. These requirements reflect one part of the tension observed in the DOJ's antitrust case against Google: the competing demands for data sharing to enhance competition and for robust data protection to safeguard privacy. Such proposals capitalize on the lack of comprehensive privacy rules to achieve distinct policy outcomes. Without a unified framework, tangentially focused bills will continue to surface at the federal level, addressing symptoms rather than the root issue: a lack of consensus and direction on data privacy.

A lack of a federal framework not only affects existing industries, but also emerging ones, such as wearable technology. In 2008, Illinois became the first state to regulate biometric information under the Illinois Biometric Information Privacy Act (BIPA), which has been a disaster.[28] Under BIPA and other similar laws, visual wearable technology designed to help visually impaired Americans "see" have been held to a strict-liability standard and have been subject to private right of action clauses that have created a "de facto ban on accessibility features."[29] When the Illinois Supreme Court ruled in 2019 that consumers could be aggrieved under BIPA even if they suffered no harm, the law spawned hundreds of lawsuits that chilled technology innovation and business formation, effectively blocking many companies from filling pressing market needs in areas of high consumer demand, including those for disabled communities. Rather than abandon that approach to data privacy, seven states and New York City have enacted their own biometric privacy laws and eight more are considering similar approaches.

[26] S. 2992 — American Innovation and Choice Online Act, Introduced October 18, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/2992/text.
[27] Amy Bos, "Importing Stagnation: How AICOA Would Kneecap American Innovation Dominance," NetChoice, January 21, 2026, https://netchoice.org/importing-stagnation-how-aicoa-would-kneecap-american-innovation-dominance/.
[28] ACLU Illinois, "Biometric Information Privacy Act (BIPA), Last updated August 26, 2025, https://www.aclu-il.org/campaigns-initiatives/biometric-information-privacy-act-bipa/; and Logan Kolas, "Key Principles for State Data Privacy Laws," The Buckeye Institute Policy Report, October 2023, https://www.buckeyeinstitute.org/library/docLib/2023-10-Key-Principles-for-State-Data-Privacy-Laws-policy-report.pdf.
[29] Bryce Chinault and Taylor Barkley, "Beyond the Screen: Wearable AI and State Policy," Abundance Institute, February 2026, https://abundance.institute/our-work/beyond-the-screen-wearable-ai-and-state-policy.

All nineteen comprehensive state data privacy laws include more restrictive regulations on sensitive data, including healthcare data. More than half of those states use expansionary definitions of consumer health data that includes commonly collected data by wearable technology devices, such as heart rate data, which is used to monitor and improve health outcomes.[30] Although it's unclear whether these data privacy laws include neural data, which is often collected to help monitor sleep, California, Colorado, Connecticut, and Montana have all amended existing data privacy statutes specifically to include neural data.[31] Maryland prohibits the sale of health data altogether—including in targeting advertising—even when there is consumer consent, thereby overriding consumer choice and violating basic principles of data privacy governance.[32] None of this bodes well for the "booming" wearable medical device market.[33]

Neither regulating data use as a secondary consideration at the federal level nor letting state data privacy laws run rampant is pro-consumer or pro-innovation. Congress must provide certainty by establishing a pre-emptive national framework, less the United States privacy leviathan continue to grow uncontrolled and unmitigated, jeopardizing current and future American innovation.

Conclusion

Even as Congress tries to move past data privacy debates, its inability to compromise on federal data privacy legislation continues to plague current technology policy discourse. Rather than doubling down on shoddily written federal privacy policies that try to create policy designs from scratch, Congress should—and must—build the debate on what works: Tennessee's data privacy law is a prime example.

Adopting Tennessee's framework—and then modifying it to include guardrails on expansive agency powers and account for AI and emerging technologies—could limit agency overreach and put Congress back in the drivers' seat on data governance.

Such an action would eliminate or inform subsequent debates on child protection, AI regulations, agency authority, national security, and antitrust remedies. An appropriately designed federal framework would also signal to the courts its vision of data protection and consumers rights, clarifying intent and reducing judicial confusion. By providing that clarity, Congress would streamline what has been a shoddily administered piecemeal approach to data governance and consumer protection. In a digital world that runs on data, Congress must rise to the challenge of providing a cohesive and forward-looking framework. One that is not merely a safeguard for the present, but an investment in a more secure, competitive, and innovative future for consumers. The history of data privacy has shown that ignoring the problem won't make it go away.

[30] Jennifer Sheridan, "Is a HIPAA-style De-identification Standard Emerging in US State Laws?" International Association of Privacy Professionals (IAPP), November 26, 2025, https://iapp.org/news/a/is-a-hipaa-style-de-identification-standard-emerging-in-us-state-laws-.
[31] Ibid.
[32] Ibid.
[33] Shane Tews, "The Wearable Revolution: Transforming Healthcare with AI-Driven Insights," American Enterprise Institute, January 15, 2025, https://www.aei.org/technology-and-innovation/the-wearable-revolution-transforming-health-care-with-ai-driven-insights/.

theamericanconsumer.org