Center for American Progress
1333 H Street NW, Suite 100E
Washington, DC 20005
202.682.1611
americanprogress.org

April 7, 2025

Center for American Progress Response to the House Energy & Commerce Privacy Working Group Request for Information

On February 12, 2025, the House Energy and Commerce Committee (House E&C) announced a Privacy Working Group (PWG),[1] consisting only of members of the Republican majority.[2] They stated they "strongly believe that a national data privacy standard is necessary to protect Americans' rights online" and issued this Request for Information (RFI) "to explore the parameters of a federal comprehensive data privacy and security framework."[3] The partisan approach of the PWG stands in stark contrast to the bipartisan efforts previously demonstrated by the House E&C Committee.[4] Nonetheless, we hope the PWG will take seriously the submissions to its RFI from a variety of stakeholders.

Almost every question in the PWG RFI[5] has been the subject of extensive Committee discussion over the past two decades. While the substance of the questions in the RFI are important, the positions of many experts and stakeholders across the spectrum on these questions have already been well established.[6] In fact, House E&C has held 13 data privacy hearings during the 118th Congress alone, advanced targeted data privacy legislation into law last Congress,[7] and held legislative markups on detailed federal privacy legislation through E&C subcommittees and committees in the previous two Congresses under both Republican and Democratic majorities.[8]

The PWG must also know that Big Tech and data brokers have carefully formulated answers designed to weaken consumer protections, limit accountability, and protect lucrative business models. We submit this response to the PWG's RFI to make clear that Industry Trade Associations, which include Big Tech among their key members,[9] have consistently opposed strong federal privacy legislation that would impact the business practices enabling them to maintain the kind of market concentration and power that drives the House majority's concerns about speech, censorship, and other issues.[10] Our response below outlines key issues a federal privacy framework must address and explains how Big Tech coalitions have routinely opposed meaningful reforms that would limit their power or strengthen privacy protections for Americans.

President Donald Trump has repeatedly called Big Tech a fundamental threat, a view echoed by leadership within the House Majority[11] and the E&C Committee[12]. Given the House Majority's strong support for President Trump and his agenda, we hope that the House E&C PWG will not author a federal privacy bill that serves as a giveaway to Big Tech but instead provides real privacy and security protections for the American people.

Fortunately, recent bipartisan efforts such as the American Data Privacy and Protection Act (ADPPA)[13] and the American Privacy Rights Act (APRA),[14] demonstrate that Democrats and Republicans alike are willing and able to stand strong together against the lobbying and

pressure from Big Tech and data brokers. To meet the moment, any serious federal privacy framework must include clear definitions of covered entities, clear obligations for each entity, modern definitions of personal and private data, and four baseline protections: data minimization, tightly scoped permissible purposes, universal opt out mechanisms, and provisions addressing AI harms.

Key questions from the RFI

I. A. How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?

Privacy legislation cannot truly be comprehensive until it accounts for every actor in the data ecosystem. Precisely defining all actors within the data chain ensures that no entity escapes scrutiny and no data slips through the cracks. This includes acknowledging that controllers, processors acting on their behalf, and third-party entities such as advertisers each pose distinct risks to personal privacy. As part of this, legislation must explicitly distinguish data brokers from other third parties, recognizing that their core business is solely the aggregation and sale of personal information and therefore requires a heightened level of oversight. It also means bringing government service providers into scope. These private companies, which collect, manage, or process data on behalf of government agencies, often handle highly sensitive information in areas such as public benefits, education, and law enforcement.

I. B. What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?

Clear responsibilities ensure every actor has enforceable duties and cannot shift blame or responsibility onto others. Controllers must strictly limit the collection, use, and retention of personal data, protect sensitive data, and provide users with meaningful rights and ways to exercise them, including universal opt-outs. Processors, including government service providers, must operate strictly under the direction of a controller, adhere to contractual boundaries, and be prohibited from using data for their own purposes. Third parties, entities that are not controllers or processors must face clear restrictions, including transparency about data sources and limits on further use or transfer without consent. Data brokers present uniquely high risks, and whether their business model should even be permitted to continue is an open question. At minimum, if allowed to operate, they should be required to register with a government agency, publicly disclose their practices, and be banned from facilitating fraud, harassment, or deception. They must also support universal opt-out and delete tools that give individuals real control over their data.

II. A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

A strong federal privacy law must include modern definitions that reflect how data is collected and misused today. Sensitive data must be defined broadly, covering not only traditional categories like biometric, genetic, geolocation, and health data but also private communications and personal media, browsing activity over time and across platforms, and sensitive inferences. Similarly, the definition of personal data must account for modern tracking methods by covering

information that identifies or is linked or reasonably linkable to a device that identifies or is linked or reasonably linkable to one or more individuals.

4 Baseline protections for a functional privacy framework

Given the RFI's 3,500-word limit, the below does not attempt to address every issue that a comprehensive federal privacy law must address. Instead, it focuses on the minimum core elements that are essential to any comprehensive privacy bill. These include data minimization, a narrowly tailored permissible purposes section that includes a carve-out for public interest research, opt out rights with a universal mechanism, and AI provisions. Each addresses a critical weakness in the current data ecosystem and must not be diluted to satisfy industry opposition.

While this column highlights opposition from "Big Tech," much of the sourcing comes from public positions taken by major industry trade associations that represent the interests of large technology companies. Generally, "Big Tech" refers to six dominant firms including Amazon, Apple, Alphabet, Google, Meta, and Microsoft. However, there are also other large tech and data-driven companies with significant market power that influence privacy policy debates such as TikTok, X (formerly Twitter), and Snap. We made a good-faith effort to identify and include direct statements from individual companies like Google. Microsoft, notably, has long expressed public support for comprehensive federal privacy legislation.[15] But in most cases, the interests of tech companies are represented by trade associations rather than tech companies speaking under their own names.[16] This is a strategy that seemingly allows companies to influence policy debates without direct exposure.[17] As a result, we drew from public positions taken by three major industry trade associations: the Information Technology Industry Council (ITI), TechNet, and the U.S. Chamber of Commerce. The first two list at least four of the six Big Tech companies as members, including Amazon, Apple, Google, and Meta.[18] While the U.S. Chamber of Commerce does not have traditional members in the same way, leaders from both Meta and Microsoft sit on its board of directors.[19] Because these organizations either include[20] or are publicly funded by Big Tech[21] and routinely lobby with their interest in mind, we believe it is appropriate to treat their positions as representative of the industry's stance, especially when individual companies have not offered independent public statements on the issue. This approach is necessary given the opacity of company-specific disclosures and the strategic role of trade groups to obscure direct opposition.

1. Data Minimization

Overview: Real data minimization limits companies to collecting, processing, retaining, and transferring only the minimum personal data that is necessary to provide a specific product or service requested by the individual. This includes deleting data once it is no longer needed to serve the purpose for which it was collected. Data minimization has been a foundational principle in privacy law for decades. The Privacy Act of 1974 established data minimization as a key requirement for government agencies, mandating that they only maintain information about individuals if it is directly relevant and necessary to fulfill a legally authorized purpose.[22] More recently, bipartisan proposals like the APRA have built on this tradition by including enforceable data minimization rules.[23]

Impact on Americans: When companies are limited to collecting only what is necessary and are required to delete data after the purpose for which it was collected is accomplished, Americans gain critical protections against a range of privacy harms. Limiting data collection reduces profiling, preventing companies from using detailed personal and behavioral data such as demographic information and browsing history to categorize individuals unfairly. It also curtails commercial exploitation, stopping businesses from extracting and monetizing intimate personal details like location history. Additionally, strict limits on data collection combats online surveillance, ensuring that individuals are not continuously tracked across platforms, reducing the risk of intrusive monitoring by commercial entities. Similarly, reducing the volume and sensitivity of stored data helps decrease the harms caused by potential breaches. It also helps ensure that people aren't forced to give up unnecessary personal information to access basic products or services, such as providing their full date of birth just to read a standard news article.

Opposition from Industry Trade Associations and Big Tech: Big Tech companies like Google often advocate for principles-based frameworks that give organizations discretion to determine what responsible data practices look like in their specific context.[24] In a recent white paper, Google promoted a “responsible data practices” model that includes data minimization as one strategy to reduce risk, defined as limiting collection, use, and disclosure to what is “reasonably necessary and proportionate” for providing a product or service.[25] However, the paper does not address limits on data retention, nor does it clarify whether “disclosure” includes the sale or transfer of data to third parties. This model allows companies to determine for themselves what data is necessary or proportionate, based on internal risk assessments and business needs. By resisting clear limits on data practices, Big Tech is able to preserve business strategies that depend on expansive and ongoing data collection. For instance, social media platforms continuously track user activities, such as likes and browsing patterns, to build detailed behavioral profiles used for targeted advertising. These practices are precisely what meaningful data minimization requirements are designed to curb.

2. Narrowly Tailored Permissible Purposes (with public interest research carve out)

Overview: A strong permissible purposes section must narrowly define exceptions to data minimization rules. These exceptions should allow data use beyond providing a requested service only when it serves a clear public benefit or is necessary for basic operations. This means avoiding vague or overly broad justifications, such as generic appeals to innovation or efficiency, which can be stretched to justify nearly any kind of data processing. Legislation should include essential carve-outs for areas like public safety, but these must be carefully defined to avoid misuse. Critically, any provision that allows data to be shared with law enforcement must be limited to data that was legally collected in the first place, and only shared under a valid legal process, such as a warrant. Companies should not be permitted to collect data solely on the basis that it might someday be useful to law enforcement. Carve-outs for fraud, harassment, public safety incidents, or criminal activity should prohibit both the sale or transfer of data to government entities for payment or other consideration, as well as any voluntary sharing of data. Ambiguous terms like "public safety" or "criminal activity" must be

tightly defined so that they cannot be used to justify surveillance of lawful behavior, such as peaceful protest or political organizing.

A public interest research carve-out is essential to ensure researchers can access the data needed to study how digital platforms, AI systems, and other technologies impact society. Importantly, this access must extend beyond de-identified data, which often lacks the detail and structure required to identify patterns of harm. CAP raised this concern in a letter to Committee leadership in response to the APRA discussion draft,[26] and the Committee appropriately addressed it during markup by removing the restriction to de-identified data.[27] This revision ensures researchers can obtain more meaningful data under secure and lawful conditions. Access of this kind is vital for analyzing platform dynamics, algorithmic systems, and their effects on areas like public health, civic participation, and safety. Enabling this kind of research allows policymakers and the public to better understand how these systems operate, laying the groundwork for smarter, more effective regulation. Without this carve-out, companies can use a privacy law as a shield to block legitimate research.

Impact on Americans: Narrowly defining permitted purposes offers stronger protection against misuse and exploitation by companies. Ambiguous terms like "public safety" and “criminal activity” can be stretched to justify invasive surveillance practices, often without people’s knowledge or consent. By clearly restricting the circumstances under which data can be used for law enforcement or shared with government agencies, a well-constructed permitted purposes section prevents companies from creating backdoor channels to hand over data without legal accountability—for example, collecting data under the guise of investigating a public safety incident and later sharing it voluntarily with law enforcement without a warrant or legal process. Additionally, a strong research carve-out ensures that privacy laws do not block the ability of independent researchers to uncover harms and inform better public policy.

Opposition from Industry Trade Associations: Industry coalitions have supported broad and loosely defined permissible purposes. ITI’s proposed privacy framework allows companies to justify data use based on subjective risk assessments rather than clear legal limits. For example, it considers a use as “legitimate” if the privacy risk is deemed negligible or is minimized to a reasonable level, or if the perceived benefits outweigh any potential harm.[28] These determinations are left to the judgment of the companies themselves, meaning that data collection and processing could proceed based on internal calculations of “acceptable” risk or benefit. Additionally, its “public interest uses” list includes broad and ambiguous purposes, such as “facilitating the efficient distribution of websites and other internet content.”[29] TechNet even opposes strong limits on government use of third-party data.[30] These positions collectively seek to preserve the status quo or even expand it by allowing companies to stretch permitted purpose exceptions to fit their current practices, rather than accept narrowly tailored rules that protect individuals and prevent abuse.

3. Opt Out Rights and Universal Mechanism

Overview: A universal opt-out mechanism allows individuals to communicate their privacy preferences—such as opting out of targeted advertising or the sale of sensitive data—across

multiple websites and services with a single action.[31] These mechanisms include tools such as browser settings or extensions that send automated signals, like the Global Privacy Control (GPC), to notify companies of the user's intent to opt out.[32] Covered entities should be required to honor these signals in order for them to have meaningful effect. Without such mechanisms, individuals are left to manage opt-outs manually, which often requires navigating different privacy policies, interfaces, and account settings across hundreds of services. A universal mechanism provides a uniform standard for both consumers and businesses, making privacy choices easier to exercise and implement.

Impact on Americans: Without a universal opt-out mechanism, Americans are forced to manage their privacy settings individually across hundreds of websites, apps, and services. This process is time-consuming and inaccessible for many people, especially those who lack the technical skills to navigate complex interfaces. The result is that, in practice, many people are effectively denied the ability to exercise rights that may exist on paper. For lawmakers who are committed to restoring control to consumers and enhancing trust in online services, supporting universal opt-out is a critical step toward achieving that goal.

Opposition from Industry Trade Associations: By enabling individuals to limit data collection and sharing across multiple platforms through a single, consistent action, it would make it far easier for users to avoid widespread tracking. This threatens the scale and efficiency of the data-driven business practices many companies depend on. Industry coalitions often claim that implementing such mechanisms would be technically complex or overly burdensome. However, even Google has acknowledged that overwhelming users with constant consent requests can lead to "consent fatigue," where people stop paying attention and click "agree" without thinking.[33] Although this argument was made in opposition to broad opt-in requirements, the same concern likely applies to opt-outs as well and highlights the value of simpler, user-friendly mechanisms like universal opt-out.

4. AI Prohibitions

Overview: Artificial Intelligence systems rely on vast amounts of personal data, often collected and processed in ways that individuals cannot fully understand or control. Privacy legislation must explicitly account for AI-related risks and harms, recognizing that data regulation alone is insufficient to mitigate the most dangerous applications of AI. A strong federal privacy framework should not only govern data practices that fuel these systems but also establish clear guardrails against their misuse. Certain high-risk AI applications—such as automated job termination, real-time biometric surveillance, and social scoring—pose direct threats to civil liberties, economic security, and democratic norms and must be restricted outright. Federal privacy legislation must not preempt states from enacting or enforcing bans on such applications, as states play a critical role in responding to local risks, addressing emerging harms, and upholding individual rights – even where Congress has shown itself unable or unwilling to act.

Impact on Americans: Without prohibitions for the most damaging, high-risk uses of AI, Americans will be susceptible to irreversible decisions that directly worsen their livelihoods.

Americans risk living in a society where opaque algorithms make consequential decisions without accountability, diminishing individual freedoms. Establishing firm boundaries for prohibited practices ensures that AI serves the public good rather than amplifying harm and helps balance the crucial tradeoff between harnessing AI's good and mitigating its bad. If a federal privacy law preempted state law and prevented states from taking action against high-risk AI systems, Americans could be left vulnerable to unregulated mass surveillance, algorithmic discrimination, and unchecked corporate power over employment and financial stability.

Opposition from Industry Trade Associations: Industry coalitions have resisted strong AI prohibitions, arguing that restrictions should only apply to narrowly defined, high-risk use cases.[34] TechNet, for example, opposes blanket bans or moratoriums on technologies like facial recognition or biometric systems, except where there is a specific, unacceptably high risk case identified and the legislation is narrowly tailored to address that unacceptably high risk.[35] They push for a harm-based threshold that requires clear, demonstrable evidence of unacceptable risk before any regulation can occur.[36] At the same time, these groups also seek to weaken enforcement mechanisms by promoting the inclusion of loopholes such as the right to cure, rebuttable presumptions, and affirmative defenses.[37] This combination of narrow definitions and diluted enforcement would leave the most harmful AI applications largely unchecked.

Conclusion

The House E&C RFI may appear to reflect a genuine interest in advancing privacy legislation, but the questions it poses fail to move the conversation forward in any meaningful way. These are not new or unresolved issues; they are foundational issues that have been discussed and refined by experts for years. What's needed now is not another delay, but a bipartisan and comprehensive federal privacy law that puts people over profits and stands up to the relentless lobbying of Big Tech and data brokers. Lawmakers should anchor any federal privacy law in the baseline protections outlined here, which reflect the real concerns of the public.

The positions of American Progress, and our policy experts, are independent, and the findings and conclusions presented are those of American Progress alone. A full list of supporters is available here.

---

[1] House Committee on Energy & Commerce, "Chairman Guthrie and Vice Chairman Joyce Announce Creation of Privacy Working Group," Press release, February 12, 2025, available at https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-announce-creation-of-privacy-working-group.

[2] Ibid.

[3] House Committee on Energy & Commerce, "Privacy Working Group Request for Information," available at https://d1dth6e84htgma.cloudfront.net/02_21_2025_PWG_Request_for_Info_2_e1753e1356.pdf (last accessed April 2025).

[4] House Committee on Energy & Commerce, "House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill," Press release, June 3, 2022, https://energycommerce.house.gov/posts/house-and-senate-leaders-release-bipartisan-discussion-draft-of-comprehensive-data-privacy-bill; House Committee on Energy & Commerce, "Committee Chairs Rodgers, Cantwell Unveil Historic Draft Comprehensive Data Privacy Legislation," Press release, April 7,

2024, available at https://energycommerce.house.gov/posts/committee-chairs-rodgers-cantwell-unveil-historic-draft-comprehensive-data-privacy-legislation.

[5] House Committee on Energy & Commerce, "Privacy Working Group Request for Information."

[6] David Brody, "STATEMENT OF DAVID BRODY MANAGING ATTORNEY OF THE DIGITAL JUSTICE INITIATIVE LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW U.S. HOUSE COMMITTEE ON ENERGY AND COMMERCE INNOVATION, DATA, AND COMMERCE SUBCOMMITTEE HEARING ON LEGISLATIVE SOLUTIONS TO PROTECT KIDS ONLINE AND ENSURE AMERICANS' DATA PRIVACY RIGHTS," April 17, 2024, available at https://www.lawyerscommittee.org/wp-content/uploads/2024/04/David-Brody-Lawyers-Committee-House-EC-Cmte-Written-Testimony-4-17-24-PM-Final.pdf; Caitriona Fitzgerald, "Hearing on 'Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security,'" June 14, 2022, available at https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf.

[7] Protecting Americans' Data from Foreign Adversaries Act of 2024, Public Law 118-50, 118th Cong., 2nd sess. (April 24, 2024), available at https://www.congress.gov/118/plaws/publ50/PLAW-118publ50.pdf.

[8] American Data Privacy and Protection Act, H.R.8152, 117th Cong., available at https://www.congress.gov/bill/117th-congress/house-bill/8152/all-info; House Committee on Energy & Commerce, "Full Committee Hybrid Markup," July 20, 2022, available at https://www.congress.gov/117/meeting/house/115041/documents/HMKP-117-IF00-20220720-SD003.pdf; House Committee on Energy & Commerce, "Subcommittee on Innovation, Data, and Commerce Markup," May 23, 2024, available at https://www.congress.gov/118/meeting/house/117372/documents/HMKP-118-IF17-20240523-SD035.pdf.

[9] Information Technology Industry Council (ITI), "ITI Members," available at https://www.itic.org/about/membership/iti-members (last accessed April 2025), ITIC includes in their members Amazon, Apple, Google, Meta, and Microsoft; Computer & Communications Industry Association (CCIA), "Members," available at https://ccianet.org/about/members/ (last accessed April 2025), CCIA includes in their members Amazon, Apple, Google, and Meta; TechNet, "Members," available at https://www.technet.org/our-story/members/ (last accessed April 2025), TechNet includes in their members Amazon, Apple, Google, and Meta; U.S. Chamber of Commerce, "U.S. Chamber Board of Directors," available at https://www.uschamber.com/about/governance/board-of-directors (last accessed April 2025), While the U.S. Chamber of Commerce does not have traditional members, leaders from both Meta and Microsoft sit on its board of directors.

[10] House Committee on Energy & Commerce, "Communications and Technology Subcommittee Hearing: "Preserving Free Speech and Reining in Big Tech Censorship," March 28, 2023, available at https://energycommerce.house.gov/events/communications-and-technology-hearing-titled-preserving-free-speech-and-reining-in-big-tech-censorship; House Committee on Energy & Commerce, "E&C Republican Leaders Demand White House Share their Big Tech Censorship Correspondences," Press release, September 13, 2022, available at https://energycommerce.house.gov/posts/e-and-c-republican-leaders-demand-white-house-share-their-big-tech-censorship-correspondences; Speaker Mike Johnson, Facebook, September 5, 2024, available at https://www.facebook.com/story.php?story_fbid=pfbid025ex6RmSpNWeiG9FU95TxqjzFfig9pnk9Sd9jHSXRxgLJPVunXHQWLpQ1VMbbF9KMl&id=100044249298524; Jim Jordan and others, "Letter to Mark Zuckerberg," Congress of the United States, House of Representatives, Committee on the Judiciary, July 22, 2021, available at https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2021-07/2021-07-22-JDJ-MJ-DB-to-Zuckerberg-re-Gov-Censor.pdf.

[11] Alexis Keenan, "Trump isn't backing down from Big Tech fights — but is willing to bend on AI," March 25, 2025, *Yahoo! Finance*, available at https://finance.yahoo.com/news/trump-isnt-backing-down-from-big-tech-fights--but-is-willing-to-bend-on-ai-140032980.html; Alexis Keenan, "Trump just gave a new signal he isn't going to let up on Big Tech," *Yahoo! Finance*, December 5, 2024, available at https://finance.yahoo.com/news/trump-just-gave-a-new-signal-he-isnt-going-to-let-up-on-big-tech-152023282.html; *Fox Business*, "Trump slams Google over alleged censorship: They're going to be close to shut down," August 2, 2024, available at https://www.youtube.com/watch?v=L7BuDtQucgA; Jing Pan, "'They've been very irresponsible': Donald Trump warned Google will be 'close to shut down' — now the Justice Department considers breaking up the search engine giant," *Moneywise*, October 16, 2024, available at https://moneywise.com/news/economy/donald-trump-warned-google-will-be-close-to-shut-down-now-the-justice-department-considers-breaking-up-the-search-engine-giant; Nicholas Reimann, "Trump Slams Big Tech 'Corruption' As Stock Behind His Truth Platform Tumbles (Again)," *Forbes*, April

21, 2022, available at https://www.forbes.com/sites/nicholasreimann/2021/10/26/trump-slams-big-tech-corruption-as-stock-behind-his-truth-platform-tumbles-again/; Sonam Sheth, "What Donald Trump Has Said About Mark Zuckerberg," *Newsweek*, November 27, 2024, available at https://www.newsweek.com/what-donald-trump-has-said-about-mark-zuckerberg-1992843; Timothy Nerozzi, "Trump blasts Meta and Google after users claim companies censored assassination attempt searches," *Fox Business*, July 30, 2024, available at https://www.foxbusiness.com/politics/trump-blasts-meta-google-after-users-claim-companies-censored-assassination-attempt-searches.

[12] Congressman Brett Guthrie, "December 3, 2021 newsletter," December 3, 2021, available at https://guthrie.house.gov/news/email/show.aspx?ID=S2EN6Z23TX77XBBWA73M2AX53E; Brennan Crain, "Guthrie seeks input from people ahead of hearing with Big Tech CEOs," March 23, 2021, *WCLU News,* available at https://www.wcluradio.com/2021/03/23/guthrie-seeks-input-from-people-ahead-of-hearing-with-big-tech-ceos/; Congressman John Joyce, "Dr. Joyce Pushes for Answers on Censorship, Conservative Bias from Big Tech," *Press release*, May 5, 2021, available at https://johnjoyce.house.gov/media/in-the-news/dr-joyce-pushes-answers-censorship-conservative-bias-big-tech; Congressman John Joyce, "Dr. Joyce: Big Tech Censorship Won?t Stop with President Trump," *Press release*, May 5, 2021, available at https://johnjoyce.house.gov/media/in-the-news/dr-joyce-big-tech-censorship-wont-stop-president-trump.

[13] House Committee on Energy & Commerce, "House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill."; American Data Privacy and Protection Act, H.R.8152.

[14] House Committee on Energy & Commerce, "Committee Chairs Rodgers, Cantwell Unveil Historic Draft Comprehensive Data Privacy Legislation."; House Committee on Energy & Commerce, "Subcommittee on Innovation, Data, and Commerce Markup."; American Privacy Rights Act of 2024, H.R. 8818, 118th Cong., 2nd sess. (May 21, 2024), available at https://docs.house.gov/meetings/IF/IF17/20240523/117372/BILLS-118pih-HR____AmericanPrivacyRi.pdf.

[15] Microsoft, "Microsoft Advocates Comprehensive Federal Privacy Legislation," *Press release*, November 3, 2025, available at https://news.microsoft.com/2005/11/03/microsoft-advocates-comprehensive-federal-privacy-legislation/; Alfred Ng, "Microsoft wants a US privacy law that puts the burden on tech companies," *CNET*, May 20, 2019, available at https://www.cnet.com/news/politics/microsoft-wants-a-us-privacy-law-that-puts-the-burden-on-tech-companies/.

[16] Amelia Minkin and Michael Beckel, "Big Tech Ramps Up Lobbying as Industry Seeks to Thwart Legislation to Protect Kids Online" (Washington: Issue One, October 22, 2024), available at https://issueone.org/articles/big-tech-ramps-up-lobbying-as-industry-seeks-to-thwart-legislation-to-protect-kids-online/; David McCabe, "Tech lobby outlines its own set of privacy regulations," *Axios*, October 22, 2018, available at https://www.axios.com/2018/10/22/iti-privacy-framework-1540156635; SEC filing from Boston Common Asset Management, "Alphabet Inc. Proposal 5 on the Company's 2022 Proxy Statement," May 18, 2022, available at https://www.sec.gov/Archives/edgar/data/1409427/000121465922007183/p518221px14a6g.htm, the proposal states "Alphabet belongs to the Chamber of Commerce" as part of a shareholder proposal to require "Alphabet to prepare an annual report on its lobbying expenditures."

[17] Matt Weinberg, "New tech trade associations will have big role in future tech policy," *TechCrunch*, May 2, 2017, available at https://techcrunch.com/2017/05/02/new-tech-trade-associations-will-have-big-role-in-future-tech-policy/.

[18] [18] Information Technology Industry Council (ITI), "ITI Members," ITIC includes in their members Amazon, Apple, Google, Meta, and Microsoft; Computer & Communications Industry Association (CCIA), "Members," CCIA includes in their members Amazon, Apple, Google, and Meta; TechNet, "Members," TechNet includes in their members Amazon, Apple, Google, and Meta.

[19] U.S. Chamber of Commerce, "U.S. Chamber Board of Directors."

[20] SEC filing from Boston Common Asset Management, "Alphabet Inc. Proposal 5 on the Company's 2022 Proxy Statement," showing Alphabet as part of US Chamber of Commerce as of 2022.

[21] Tech Transparency Project, "Find Out Which Groups Get Big Tech Funding," August 10, 2021, available at https://www.techtransparencyproject.org/articles/find-out-which-groups-get-big-tech-funding (last accessed April 2025), this dataset shows ITI, CCIA, TechNet are funded by various Big Tech companies; Microsoft, "Microsoft US Government Affairs Trade Association (501c6) Memberships FY24," available at https://cdn-dynmedia-

1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/FY24-Trade-Association-Memberships.pdf, shows Microsoft is a member of the U.S. Chamber of Commerce and ITI.
[22] Legal Information Institute, "5 U.S. Code § 552a - Records maintained on individuals," available at https://www.law.cornell.edu/uscode/text/5/552a (last accessed April 2025).
[23] American Privacy Rights Act of 2024, H.R. 8818.
[24] Google, "Google Responsible Data Practices," available at https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Responsible_Data_Practices.pdf (last accessed April 2025).
[25] Ibid.
[26] Nicole Alvarez, "CAP Authors Letter Addressing Public Interest Research in the American Privacy Rights Act" (Washington: Center for American Progress, May 30, 2024), available at https://www.americanprogress.org/article/cap-authors-letter-addressing-public-interest-research-in-the-american-privacy-rights-act/.
[27] American Privacy Rights Act of 2024, H.R. 8818. https://www.congress.gov/bill/118th-congress/house-bill/8818/text
[28] Information Technology Industry Council (ITI), "Framework to Advance Interoperable Rules (FAIR) on Privacy," https://www.itic.org/dotAsset/feb6ab98-7c3b-421b-9f92-27528fa4c4f2.pdfavailable at https://www.itic.org/dotAsset/feb6ab98-7c3b-421b-9f92-27528fa4c4f2.pdf (last accessed April 2025).
[29] Ibid.
[30] TechNet, "Privacy and Security," January 1, 2025, available at https://www.technet.org/policy/privacy-and-security/ (last accessed April 2025).
[31] Nathalie Maréchal and Nick Doty, "Meaningful Opt-Out Rights Require Companies to Do Their Part. State Governments Might Have to Make Them" (Washington: Center for Democracy and Technology, March 3, 2025), available at https://cdt.org/insights/meaningful-opt-out-rights-require-companies-to-do-their-part-state-governments-might-have-to-make-them/.
[32] Nick Doty, "It's Time to Standardize the Global Privacy Control" (Washington: Center for Democracy and Technology, December 13, 2023), available at https://cdt.org/insights/its-time-to-standardize-the-global-privacy-control/.
[33] Google, "Google Responsible Data Practices."
[34] TechNet, "Privacy and Security."
[35] Ibid.
[36] Ibid.
[37] TechNet, "Artificial Intelligence," January 1, 2025, available at https://www.technet.org/policy/state-artificial-intelligence/ (last accessed April 2025).