



**Testimony of Joel Thayer
President of Digital Progress Institute
Before the
The U.S. Senate Judiciary Privacy, Technology, and the Law
“Protecting the Virtual You: Safeguarding Americans’ Online Data”
Wednesday, July 30, 2025**

Thank you, Chairwoman Blackburn, Ranking Member Klobuchar, and esteemed members of this committee, for inviting me to testify and holding this important hearing.

My name is Joel Thayer, and I am the president of the Digital Progress Institute—a think tank based in Washington, D.C. focused on advancing bipartisan policies in the tech and telecom space. Ensuring privacy for all is a founding principle of the Institute and, as such, I very much appreciate this committee’s commitment to building out a privacy framework that further assures that the integrity and ownership of our digital selves remains in our domain; not by companies with a domain name.

The concept of privacy is foundational to our constitutional democracy. Indeed, the Fourth Amendment prevents unlawful searches and seizures.¹ The Fifth Amendment prevents self-incrimination.² The First Amendment prevents the government from compelling Americans from making disclosures.³ Some states, like Montana, explicitly list the right to privacy in their constitutions.⁴

Although our right to privacy from our government is well established, that is unfortunately not the case with respect to companies. With the allure of free services, we provide details about our most intimate selves to trillion-dollar tech companies who, in turn, make an enormous profit off the data they collect.

They know everything about us. What we like to eat. When we sleep. Where we live. Where we are. Our beliefs. Our fears. Curiously, they claim our age confounds them, but let’s set that aside.

¹ U.S. Const. amend IV.

² *Id.* at amend. V.

³ *NAACP v. Alabama*, 357 U.S. 449 (1958) (holding that the First Amendment protected the free association rights of the National Association for the Advancement of Colored People and its members).

⁴ Mont. Const. art. II, § 10.

Worse, a recent Pew Study shows that 73% of Americans feel they have limited to no control over how companies use their personal information.⁵ And the reality is they don't. We sign privacy policies that are filled with so much legal jargon that it may as well be unintelligible to the average person and—presto!—our data is now their data.

The problem is not just that they sell our data to third-party advertisers but also to those who use our data to create fake images, curate biased newsfeeds, conduct elaborate scams, and even engage in espionage. In short, we are not in control, and Americans are right to be concerned.

And with the advent of AI, this trend will only increase.

It makes the need for a national privacy framework preeminent because our current system is unsustainable. Even though many states, like California and Texas, have passed comprehensive privacy laws, we still need federal action to ensure we hold these companies accountable.

To be sure, tech behemoths view privacy violations as a mere cost of doing business, with penalties akin to a parking violation given their bottomless coffers. To demonstrate how some privacy laws have been of little help to consumers, let's get specific. Consumers sued Apple under California's privacy law, in part, for sharing recorded conversations that included personal health information with their physicians to medical ad companies.⁶ Apple's surveillance and recordings covered conversations spanning a little under a decade. The case settled. So, what was the total cost of Apple giving advertisers an inside perspective on doctor-patient relations? A meager \$95 million, which accounts for about 9 hours of Apple's annual profit.⁷ And consumers won't see about a third of that, as it's reserved for the lawyers.

The reality is that if these Big Tech companies cared about user privacy, they would protect it. For instance, Google,⁸ Amazon,⁹ and Apple¹⁰ can stop lowering their privacy protocols for autocratic regimes, such as the Chinese Communist Party, that seek to use their platforms to spy on consumers. Even better, Google can simply stop manipulating users' privacy settings on their devices and third-party services, which is already illegal.¹¹ Meta could stop unlawfully capturing

⁵ Colleen McClain, Michelle Faverio, Monica Anderson, & Eugenie Park, *How Americans View Data Privacy*, Pew Research (Oct. 18, 2023), <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.

⁶ *Lopez, et al v. Apple Inc.*, No. 19-04577, (N.D. Cal); see also, *Lopez, et al v. Apple Inc.*, No. 4:19-cv-04557-JSW, Second Amended Complaint, Doc. No. 70, paras. 38-43 (Mar. 17, 2021).

⁷ Jonathan Stempel, *Apple to Pay \$95 Million to Settle Siri Privacy Suit*, Reuters (Jan. 2, 2025), <https://www.reuters.com/legal/apple-pay-95-million-settle-siri-privacy-lawsuit-2025-01-02/>.

⁸ Jack Poulson, *I Used to Work for Google. I Am a Conscientious Objector*, N.Y. Times (Apr. 23, 2019), <https://www.nytimes.com/2019/04/23/opinion/google-privacy-china.html>.

⁹ Steve Stecklow & Jack Dastin, *Amazon Partnered with China Propaganda Arm*, CNBC (Dec. 17, 2021), <https://www.cnbc.com/2021/12/17/amazon-partnered-with-china-propaganda-arm.html>.

¹⁰ *Inside Apple's Compromises in China: A Times Investigation*, N.Y. Times (Jun. 17, 2021), <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html>.

¹¹ *In re Google Assistant Privacy Litigation*, No. 19-cv-04286-BLF (N.D. CA 2024), <https://www.googleassistantprivacylitigation.com/> (alleging that Google Assistant can activate and record communications even when a user does not intentionally trigger Google Assistant with a hot word, like "Okay

and using personal biometric data.¹² Apple describes user privacy as a “human right,” but, in reality, it treats user privacy less as a fundamental human right and more as a license to collude with Google and other Big Tech firms to monetize and monopolize every facet of its users’ data, lives, and privacy.

It is no wonder why that 85% of people want more to be done to protect user privacy.¹³ We need government intervention here.

The good news is that protecting privacy is a bipartisan issue. Indeed, 20 states across the political spectrum have passed privacy laws. And, as evidenced by this hearing, Congress appears poised to address the issue again. The Institute welcomes this much-needed development.

With that in mind, here are a few high-level suggestions as the Committee evaluates paths forward:

First, define your goals and keep the framework targeted at accomplishing its goals. One of the primary issues with previous attempts at passing meaningful privacy laws has been that bills attempt to do too much all at once. We have seen the most success in legislation that has clearly articulated goals with targeted solutions. It is why the Institute has supported targeted, bipartisan measures, such as the Protecting Americans from Foreign Adversary Controlled Applications Act, TAKE IT DOWN Act, Kids Online Safety Act, and App Store Accountability Act to name a few.

As we have seen in the E.U.’s General Data Protection Regulation (GDPR), overly sweeping privacy laws have the unintended consequence of entrenching incumbents. The GDPR should be a cautionary tale for the U.S., because it clearly shows that privacy regulations without market guardrails can seriously exacerbate today’s competition issues we have with Big Tech. For example, the European Centre of Economic Policy Research found that “[w]ith the introduction of GDPR, the dominant firm in many markets for web technologies, Google, increases its market share whereas all other firms that supply web technology either do not see a change in market share or suffer losses...”¹⁴ The primary reason is that the tech market is highly vertically

Google,” or manually activate Google Assistant on their device); see also, Erik Sherman, *Is Google Ignoring Internet Privacy?* CBS News (Feb. 22, 2012), <https://www.cbsnews.com/news/is-google-ignoring-internet-privacy-update/>.

¹² The Office of the Attorney General of Texas, *Attorney General Ken Paxton Secures \$1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data In Largest Settlement Ever Obtained From An Action Brought By A Single State*, Press Release (Jul. 30, 2024), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture>.

¹³ Exploding Topics, *23+ Alarming Data Privacy Statistics for 2025*, Blog (Jun. 5, 2025), <https://explodingtopics.com/blog/data-privacy-stats>.

¹⁴ Peukert, C, S Bechtold, M Batikas and T Kretschmer, *DP14475 European Privacy Law and Global Markets for Data*, CEPR Discussion Paper No. 14475. CEPR Press, Paris & London (2020). <https://cepr.org/publications/dp14475>.

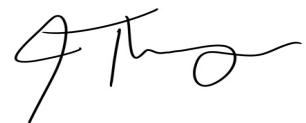
integrated where smaller companies are inextricably reliant on these larger platforms to either house their data, host their apps or even promote their services on those Big Tech platforms.

Second, enforcement matters. In our experience, agency actions or attorney general enforcement are the most effective. For instance, the Texas Attorney General recently secured a \$1.345 billion settlement against Google “for unlawfully tracking and collecting users’ private data regarding geolocation, incognito searches, and biometric data.”¹⁵ As should be obvious, that’s \$1.345 billion that *only* covers the people of Texas. Contrast that with the Apple case discussed earlier with a settlement of only \$95 million covering the entire country. In other words, a private right of action may behave more as a carrot as opposed to a stick given these companies seemingly endless teams of lawyers and budgets. What’s more, agencies can tailor their remedies more precisely to protect American citizens. For example, COPPA permits the Federal Trade Commission to promulgate rules and impose injunctive relief to enjoin certain data collection with respect to users under the age of 13.¹⁶ The Institute strongly encourages the committee to evaluate those options and possibly targeted agency rulemakings so as to prevent the overly prescriptive technical statutes.

Third, the broader the federal statute, the more important preemption will become. That’s because targeted legislation is less likely to run into differing state regimes, whereas 20 states have now passed some form of comprehensive privacy legislation. The Institute recommends that any preemption framework should be clear on what it is preempting and should reserve rights for state attorney general enforcement. Key areas ripe for preemption are developing basic definitions (*e.g.*, “personal information”), the creation of data rights, and what specific data management practices are to be prohibited.

Once again, I would like to thank the sub-Committee for allowing me to testify and I welcome any questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read 'J Thayer', with a stylized, cursive script.

Joel L. Thayer
President & Member of the Board

¹⁵ The Office of the Attorney General of Texas, *Attorney General Ken Paxton Secures Historic \$1.375 Billion Settlement with Google Related to Texans’ Data Privacy Rights*, Press Release (May 9, 2025), <https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-historic-1375-billion-settlement-google-related-texans-data>.

¹⁶ 15 U.S.C. § 57a; *see also* 15 U.S.C. § 6502.