Testimony of Joel Thayer
President of Digital Progress Institute
Before the
The Texas House Committee on the Delivery of Government Efficiency
Wednesday, August 19, 2026

Thank you, Rep. Capriglione, 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 seizers.[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 its Constitution.[4]

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

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.

Worse, a recent Pew Study shows that 73% of Americans feel they have limited to no control over how companies utilize their personal information.[5] And the reality is they don't. We sign

---

[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.
[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/.

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 along with our digital selves.

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 for selling recorded conversations of personal health information with their physicians to pharmaceutical ad companies.[6] Apple's surveillance and recordings covered conversations spanning a little over 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 Apple[10] 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, companies such as Google can simply stop manipulating users' privacy settings on their devices and third-party services, which is already illegal.[11] 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.

---

[6] *Lopez et al v. Apple Inc.*, No. 19-04577, (N.D. Cal).
[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 Comprmises 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] Erik Sherman, *Is Google Ignoring Internet Privacy?* CBS News (Feb. 22, 2012), https://www.cbsnews.com/news/is-google-ignoring-internet-privacy-update/.

It is no wonder why that 85% of people want more to be done to protect user privacy.[12] Thus, we need government intervention here.

The good news is that passing a privacy law is widely bipartisan.[13] Indeed, 20 states across the political spectrum have passed comprehensive privacy laws. Last Congress, a bipartisan group of federal legislators introduced the American Privacy Rights Act. And 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 those 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 to both pass through both houses and be an effective law. It is why the Institute has supported targeted 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.

Worse, 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 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. As indicated earlier in the case involving Apple, private right of actions can behave more as a carrot as opposed to a stick given these companies seemingly endless teams of lawyers and budgets. Whereas agency actions or AG enforcement are far more effective. For instance, here in Texas, Attorney General Paxton recently secured a $1.345 billion settlement against Google "for unlawfully tracking and collecting users' private data

[12] Exploding Topics, *23+ Alarming Data Privacy Statistics for 2025*, Blog (Jun. 5, 2025), https://explodingtopics.com/blog/data-privacy-stats.
[13] U.S. Senate Committee on Commerce, Science, & Transportation, *What Others Are Saying: The American Privacy Rights Act*, Press Release (Apr. 19, 2024), https://www.commerce.senate.gov/2024/4/what-others-are-saying.
[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.

regarding geolocation, incognito searches, and biometric data."[15] What's more, 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, we must change the incentive structure of these companies from wantonly collecting unnecessary personal data. One way is to afford consumers a digital dividend for the personal information Big Tech uses to generate revenue from ads. The unfortunate circumstance of current privacy regimes is that the pecuniary penalty is a huge price tag for everyday Americans, but for a trillion-dollar tech behemoth, it's a parking ticket. Texas's $1.345 billion settlement against Google is a great triumph for Texan consumers, but even that only amounts to 0.334% of Google's (Alphabet's) 2025 annual revenue (*i.e.*, $402.84 billion), or roughly 0.302% of its trailing 12-month revenue (*i.e.*, $445.87 billion).[17] To put that in perspective, Google generates roughly $1.10 billion per day, which means $1.3 billion represents just about 1.2 days of corporate revenue.

Let's be clear, personal data is akin to oil for these companies. They are willing to pay top dollar for access to it. Google and Meta have even created the largest digital ad exchanges where they effectively treat your data similar to a stock on the Nasdaq.[18] Given this, it may be worth the committee to evaluate whether Texas consumers are entitled to dividends on those transactions.

Nobel-winning economist Milton Friedman titled his series of economic essays "[t]here's no such thing as a free lunch," and it's time for Big Tech to pay up. Make no mistake, you own your data, not Big Tech. They are not entitled to extracting billions of dollars annually from your likeness and personal data without paying you a dime.

To be abundantly clear, you can put a price tag on personal data. Indeed, Google, Apple, and Meta do every day. Albeit in the context of antitrust, Christos Makridis and I wrote out an economic model to price out the value of individual data in the Standford Technology Law Review.[19] In that article, we posit that your data is a form of currency and is the underpinning legal tender you release to tech companies in exchange for using their so-called "free" services.

---

[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.
[17] Macrotrend, *Alphabet Revenue* (last visited Aug. 18, 2026), https://www.macrotrends.net/stocks/charts/GOOG/alphabet/revenue.
[18] SENATE JUDICIARY SUBCOMMITTEE ON COMPETITION POLICY, ANTITRUST, AND CONSUMER RIGHTS, COMPETITION IN THE DIGITAL ADVERTISING ECOSYSTEM, S. HRG. 118–112 (2023) at p. 6., https://www.congress.gov/118/chrg/CHRG-118shrg53539/CHRG-118shrg53539.pdf (finding that "Ad companies have modeled their exchanges after stock exchanges that we're familiar with, like the New York Stock Exchange.").
[19] Christos A. Makridis and Joel Thayer, The Big Tech Antitrust Paradox: A Reevaluation of the Consumer Welfare Standard for Digital Markets, 27 Stan. Tech. L. Rev. 71 (2024).

There is no reason why we cannot apply those same economic principles to develop dividends owed to the consumer for Big Tech's blatant exploitation.

In sum, creating a digital dividend may go a long way into disincentivizing them from using your data because, every time they do so, it shows as a cost on their ledgers.

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