MEMO *Published December 16, 2025 · 8 minute read*

Privacy Please! Data Privacy Should Be Tech Priority #1

Ruth Whittaker

Every day, Americans give away pieces of our identity—our shopping habits, health information, what we read and lookup, and even our physical locations—often without realizing how far that data travels or who profits from it. Targeted advertising follows us everywhere, incentivizing constant surveillance of our online habits.

But advertisers aren't the only groups with an insatiable demand for data. Fraudsters and identity thieves suck up sensitive information in pursuit of financial gain. Foreign adversaries weaponize our data to manipulate public discourse and infiltrate critical systems. Even our own government uses private data collection to surveil us, sidestepping constitutional protections.

Personal data is one of the most valuable commodities in the modern economy. But data privacy protections depend entirely on where we live. Some states give people real control over their information, others offer almost none, and the federal government is MIA.

A clear, nationwide privacy standard would ensure that every American—no matter where they live—has the same right to know, control, and protect how their personal information is used. It would spur future innovation by eliminating unnecessary regulatory hurdles and increasing consumer trust. And it would move the ball forward on other policy priorities, like making artificial intelligence safer and protecting kids online.

In this memo, we argue that a federal privacy standard isn't just an important element of a tech agenda—it should be the top priority for both parties. We also make the case that Democrats risk missing a critical opportunity to reassure voters if they don't join the debate.

Why Privacy Matters

There are a host of challenges facing Congress. Why should they lead with privacy? First, it would address real harms facing consumers. Second, it would spur innovation. Finally, it eases the conversation around other policy sticking points.

Consumers face real risks when they lose control of their data.

Consumers often don't realize how far their data travels or what ripple effects come from sharing it. Data brokers vacuum up personal information, analyze it, and make it available to a wide variety of industries to inform pricing, strategy, and eligibility for products and services. For example, landlords have outsourced research into prospective renters to brokers who offer opaque personalized scores. [1] Brokers also promise health insurance companies insights into consumers by collecting information related to consumers'

lifestyles—including daily step counts, heart rates, and calorie intake from wearable devices. [2] Car insurance companies have also used data brokers' analysis of individual driving behaviors, often collected without drivers' knowledge, to determine rates. Without knowing it, our own devices can become surveillance tools.

Many other services and devices have been similarly weaponized, with even more dire consequences. In states that implemented strict abortion bans after the fall of *Roe*, women have been advised to delete period tracking apps and turn off location sharing on all devices out of fear that their data could be accessed by third parties and used for reproductive surveillance. [3] After location data was used to serve targeted anti-abortion ads to people who had visited nearly 600 different Planned Parenthood locations, advocates raised concerns that it could also be used to coordinate private harassment campaigns or criminal investigations. [4]

Widespread data collection and lax security practices also multiply opportunities for identity theft and fraud. In 2018, sensitive information for over 500 million people was exposed when hackers breached the guest reservation database of Starwood Hotels & Resorts. The database included sensitive details of previous guests, including names, addresses, passport numbers, and payment information. [5] Retaining that much sensitive information, even after transactions have closed, creates massive risk of cyberattack or inadvertent disclosure.

A federal privacy standard would significantly reduce these risks. By restricting the amount of data collected in the first place, mandating baseline protections for that data, and limiting the sale or transfer to third parties, a federal standard would make it harder for bad actors to access data and give control back to consumers.

Universal data privacy standards would promote innovation.

In addition to minimizing the risk of harm, a federal privacy standard would also create a better foundation for future innovation than the patchwork that exists today. Any business looking to operate nationwide currently must comply with 20 different state-level data privacy policies. [6] In a survey of small and medium-sized business owners, 80% reported knowing very little about data protection laws. [7] Consumers are also not likely to track different state laws when they use connected devices, phones, and wearable tech while travelling. The proliferation of different standards across the country raises costs for small businesses, making it harder for them to scale, and undermines consumers' understanding of their rights when they travel across the country.

Eliminating uncertainty for consumers can also promote innovation by increasing the adoption of new technologies. A 2022 McKinsey survey found that consumers consider the amount of personal data required to be at least as important as shipping times when considering making a purchase. [8] Another study found that consumers made 50% more purchases on connected devices they trusted than those with low levels of trust. [9] As the "internet of things" expands and artificial intelligence offers more services, a universal guarantee of data protection could make consumers more likely to adopt new products.

A federal privacy standard could also pave the way for other important safeguards.

Many other concerns driving the modern tech policy conversation could be addressed or mitigated with a comprehensive privacy policy. Currently, only children under the age of 13 benefit from a federal standard regarding the collection and treatment of personal data. [10] Letting users control what data is collected and who it's shared with would give children over 13 (and their parents) much more control over their online experiences. Minors who want to limit targeted advertising or personalized content recommendations could opt to limit the amount of personal data they share with social media platforms, for example.

Further, universal data minimization and data protection requirements could mitigate some of the risks associated with age assurance technologies. As more platforms opt to limit the content or services they make available to child users, their ability to differentiate children from adults becomes more important. But the methods they use create privacy concerns—especially if they rely on sensitive information like facial scans, credit card information, or ID checks. Universal standards for the protection of that information could help eliminate risks, increase users' trust, and make it easier for platforms to adopt child-specific safety policies.

Data protections will also address many of the concerns with artificial intelligence. Requiring developers to be transparent about the data they collect from users to train their models would increase transparency into the models themselves, which could help inform oversight of the most advanced AI systems. Giving users the ability to correct or delete their data would also make it easier to correct adverse consequence of AI decisions. For example, a renter whose housing application was denied by an AI system trained on biased or incomplete data could review the data used to make the decision and correct any inaccuracies.

The Progressive Imperative

Democrats face a steep climb when it comes to regaining voters' support. According to recent polling by Pew, Democratic voters' frustration with their party has increased since 2021, while hope in the party has sharply declined. Across the board, voters are dissatisfied with the ideas coming out of Washington—majorities say Republicans and Democrats have only a few or no good ideas. [11] Voters want action, and Democrats need to show that they have policy solutions for the issues voters care about.

When it comes to tech policy, privacy and consumer safety is one of the top concerns voters cite. Another survey from earlier this year found that 80% of American adults are concerned about the privacy of their personal information online, and 77% would support legislation to protect their data. [12] If Democrats lead on a comprehensive privacy policy, they can show voters that they understand their concerns and begin rebuilding their trust.

If Democrats miss this moment, the Republicans are poised to take it for themselves. Despite historic bipartisan cooperation on privacy issues, House Republicans have formed their own working group on data privacy with the goal of releasing a legislative framework. [13]

There is no time to waste. The status quo leaves millions of consumers unprotected online and imposes significant drag on innovation in the private sector. Advances in artificial intelligence will only increase the demand for consumer data and magnify the risks of its misuse. The longer the federal government waits to act, the more opportunities malicious actors and foreign rivals will have to exploit our vulnerabilities.

Privacy is too important to be partisan. Democratic leaders need to join the debate and make comprehensive privacy protections the top priority when it comes to tech.

ENDNOTES

1. Leiwant, Matthew Harrold. “Locked Out: How Algorithmic Tenant Screening Exacerbates the Eviction Crisis in the United States.” *Georgetown Technology Law Review*, Vol. 6, No. 276. Feb. 2022. https://georgetownlawtechreview.org/locked-out-how-algorithmic-tenant-screening-exacerbates-the-eviction-crisis-in-the-united-states/GLTR-02-2022/. Accessed 8 Dec. 2025.

2. Robeznieks, Andis. “Insurers want patients to use wearables. That could be a problem.” *American Medical Association*, 26 Aug. 2019. https://www.ama-assn.org/practice-management/digital-health/insurers-want-patients-use-wearables-could-be-problem. Accessed 8 Dec. 2025.

3. “How to Protect Yourself? A Guide to Digital Security for Abortion/Health Care Privacy” *Medium*, Advancing Justice – AAJC, 6 Oct. 2022. https://medium.com/advancing-justice-aajc/how-to-protect-yourself-a-guide-to-digital-security-for-abortion-health-care-privacy-c6383c6418c1. Accessed 8 Dec. 2025.

4. Marrinan, Cecilia. “Geofencing: The Overlooked Barrier to Reproductive Freedom” *Council on Foreign Relations*, 30 Oct. 2024. https://www.cfr.org/blog/geofencing-overlooked-barrier-reproductive-freedom. Accessed 8 Dec. 2025.

5. Schneider, Avie. “Marriott Says Up to 500 Million Customers’ Data Stolen in Breach”, *NPR*, 30 Nov. 2018. https://www.npr.org/2018/11/30/672167870/marriott-says-up-to-500-million-customers-data-stolen-in-breach. Accessed 8 Dec. 2025.

6. “Which States Have Consumer Data Privacy Laws?” *Bloomberg* Law. 7 April 2025. https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#states-with-comprehensive-data-privacy-laws. Accessed 8 Dec. 2025.

7. "EXCLUSIVE: SURVEY SAYS! Small Business Owners Concerned New Privacy Regulations Will Hurt Bottom Line." *Connected Commerce Council.* https://connectedcouncil.org/exclusive-survey-says-small-business-owners-concerned-new-privacy-regulations-will-hurt-bottom-line-2/. Accessed 8 Dec. 2025.

8. Boehm, Jim et al. "Why digital trust truly matters." *McKinsey & Company*, 12 Sept. 2022. https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters. Accessed 8 Dec. 2025.

9. Deloitte Center for Technology, Media & Telecommunications "Connected Consumer Survey 2024", Poll, 2024. https://www.deloitte.com/us/en/about/press-room/increasing-consumer-privacy-and-security-concerns-in-the-generative-ai-era.html. Accessed 8 Dec. 2025.

10. United States Code Title 16, Chapter I, Subchapter C, Part 312. National Archives Code of Federal Regulations. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312. Accessed 8 Dec. 2025.

11. Shepard, Steven, et al. "How Americans see the parties on key issues." *Pew Research* Center, 30 Oct. 2025. https://www.pewresearch.org/politics/2025/10/30/how-americans-see-the-parties-on-key-issues/. Accessed 8 Dec. 2025.

12. Ballard, Jamie. "What Americans think about privacy and U.S. government surveillance in 2025." *YouGov*, 23 June 2025. https://today.yougov.com/politics/articles/52425-what-americans-think-about-privacy-united-states-government-surveillance-in-2025-poll. Accessed 8 Dec. 2025.

13. Hendel, John. "Guthrie wants to unveil GOP privacy priorities by year's end" *PoliticoPro,* 30 Sept. 2025. https://subscriber.politicopro.com/article/2025/09/guthrie-wants-to-unveil-gop-privacy-priorities-by-years-end-00587228. Accessed 8 Dec. 2025.