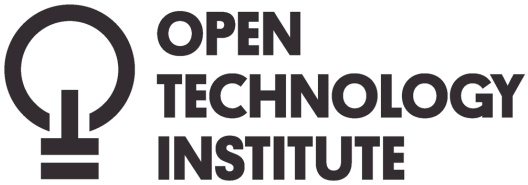

Statement of Prem M. Trivedi
Policy Director, New America's Open Technology Institute

Submitted to the

U.S. Senate Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, and Data Security

Hearing on

Strengthening Data Security to Protect Consumers
May 8, 2024

Introduction

Chair Cantwell, Ranking Member Cruz, Subcommittee Chair Hickenlooper, Ranking Member Blackburn, and Members of the Committee, thank you for the opportunity to offer testimony today on how strong data security safeguards protect consumers. A federal standard for data security, and particularly for data minimization, is critical to protecting American consumers and American companies from the over-collection of data, subsequent misuse of such data, and the harms of data breaches.

My name is Prem Trivedi, and I am the policy director of the Open Technology Institute at New America, a nonprofit and nonpartisan organization dedicated to realizing the promise of America in an era of rapid technological and social change.[1] Since 2009, the Open Technology Institute (OTI) has worked at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.[2]

OTI has long emphasized the need for strong, common federal standards in privacy and data security that protect consumers while retaining sufficient flexibility for innovation. We have been heartened to see the reemergence of a credible bipartisan legislative proposal on privacy and data security via the American Privacy Rights Act (APRA).[3] Data security and consumer privacy are two sides of the same coin. Perhaps no principle better illustrates that fundamental truth than data minimization, which requires companies to collect, use, share, and retain only what they need to provide a product or service. Strengthening federal protections for privacy and data security is vital to protecting Americans, a key foundation of responsibly regulating artificial intelligence, and an important part of safeguarding our economic and national security. We at OTI commend the Subcommittee for its leadership in spotlighting how data security and data minimization play an essential role in protecting consumers and data.

---

[1] *Our Story*, New America, https://www.newamerica.org/our-story/.
[2] *About*, New America's Open Technology Institute, https://www.newamerica.org/oti/about/.
[3] American Privacy Rights Act of 2024 (discussion draft), https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf.

My testimony makes four key points:

1. Strong data security safeguards, including data minimization, are essential to protecting consumers.
2. Consumer research shows that Americans want stronger data security and privacy laws, including the protections of data minimization.
3. Data minimization requirements in a federal privacy law could fix the broken notice and consent approach to U.S. privacy law.
4. Codifying a broader set of data security practices in federal law would also meaningfully protect consumers' and companies' data.

I. Strong Data Security Safeguards, including Data Minimization, Are Vital to Protecting Consumers

"Data minimization" may seem like a dry and technocratic-sounding term. But, at its core, it is a powerful principle for collecting, using, sharing, and retaining only the data that is necessary to provide a service or product. Data minimization is an essential element of effective privacy and data governance that protects people and organizations from misuse and mitigates the harms of data breaches. And it is already a well understood, common requirement in international, federal, and state laws and regulations. In addition, data minimization is a core part of internal company rules and risk assessments, but it is not consistently applied with sufficient rigor. A brief examination of first- and third-party tracking on the internet powerfully illustrates why we need a common national baseline for data minimization.

The average modern web page or smartphone application collects information about you—like the browser you use, your IP address, metrics about how you engage with the site or app, and any information you actively provide. This is "first-party" data collection. But a web page also uses code from other companies or entities, which are referred to as third parties—sometimes dozens of them. This type of code may be placed on a website to improve your experience or to provide a service like web analytics for the site's owner. Each of those third parties is in a position to track that site's visitors and collect and retain a broad range of data about them. If a third party's code is included on multiple websites, then you can be tracked as having visited both

pages, and data brokers can potentially bundle and sell that data to entities ranging from domestic and foreign governments to insurance companies and credit bureaus.

Even if a third party is providing a legitimate service, it is almost impossible for the average person to know if that is the case because all of this code is loaded silently in the background. Finding out which third parties a site loads requires special tools and then a further step of researching the services those third parties provide. While it might be feasible to investigate a site like senate.gov, which only loads code from two third parties, it is simply not practical to do that on very popular pages, like mainstream news websites—many of which load code from dozens of third parties. Similarly, developers of smartphone apps may include third-party libraries that can analogously track users via their devices and sometimes their activity in other apps, which is known as "cross-app tracking."

There are certainly companies in this ecosystem that follow responsible privacy practices, but many others do not show the same regard for privacy and data security. Strong data minimization rules would restrict both first-party and third-party data collection and use. They would alleviate some of the unrealistic responsibility forced onto website visitors and app users to figure out how their data is collected and used and which third parties may be tracking them. Strong rules would also bolster public trust if people knew that a federal law reasonably minimized the amount of data about them that could be gathered, used, and stored. **Companies cannot use data that they don't have.**

Cybersecurity practitioners recognize the importance of minimization. Consistent reductions in data collection and use would significantly reduce the threats posed by breaches and other security incidents. Responsible data minimization also lowers the possible harms when companies get hacked. A common data security maxim is "If you can't protect it, don't collect it."[4] A common privacy maxim is "Collect and use only what you need." And here is a synthesis that I will borrow from another civil society organization: "You don't have to protect what you don't collect."[5] This perfectly illustrates how data minimization is a cornerstone of protecting consumers and

[4] Richard Bejtlich, *New cybersecurity mantra: "If you can't protect it, don't collect it."*, Brookings, Sep. 3, 2015, https://www.brookings.edu/articles/new-cybersecurity-mantra-if-you-cant-protect-it-dont-collect-it/.
[5] John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too*, Electronic Privacy Information Center, Jun. 22, 2023, https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/.

companies, safeguarding privacy, and securing data. **Hackers cannot steal data that companies do not have.**

The central role of data minimization in data security is even clearer when we think about how some of Americans' most sensitive data is held by institutions like schools and hospitals. These organizations may have varying levels of technical capacity to implement data security measures. Although federal privacy laws cover sectors like health, finance, and education, the reality is that virtually every institution is likely to hold and use sensitive data—including data not covered by data security or privacy laws. A strictly sectoral approach to data security and privacy leaves unprotected many institutions and Americans who need a baseline level of support from a strong federal standard for data minimization and other security practices.

In addition, the need for robust data minimization and other security provisions is increasingly evident in this era of artificial intelligence (AI). The training of many AI models—particularly powerful "foundation" models designed to be adapted for a variety of purposes—requires the ingestion of huge data sets. As companies race to acquire more and more data, the pressures on privacy and data security are becoming even more acute.[6] Although there appears to be broad consensus on the need to regulate AI, public debate sometimes overlooks the fact that a baseline federal standard on privacy and data security is foundational to ethically and effectively regulating AI development.

II. Research Shows Americans Want Strong Data Security and Minimization Protections

We don't need to take data protection professionals' word about the importance of protecting data security and privacy. Consumer research by companies and nonprofits shows that Americans feel a lack of control over their data and are unsure of what data companies collect from them and how they use it. This environment of uncertainty and mistrust leaves them wanting stronger privacy and data security protections.

[6] Cade Metz, Cecilia Kang, Sheera Frenkel, Stuart A. Thompson, and Nico Grant, *How Tech Giants Cut Corners to Harvest Data for A.I*, New York Times, Apr. 8, 2024, https://www.nytimes.com/2024/04/06/technology/tech-giants-harvest-data-artificial-intelligence.html.

According to a 2023 report from the International Association of Privacy Professionals, nearly 68 percent of consumers globally said they were somewhat or very concerned about their privacy online. And only 29 percent of consumers surveyed said it was easy for them to understand how a company protects their personal data.[7] A 2023 KPMG survey of 2,000 Americans found that 86 percent of those surveyed said their data privacy is a source of growing concern.[8]

Consumers are similarly worried about data security. A 2024 Deloitte study reveals that about 60 percent of survey respondents worry that their devices are vulnerable to security breaches and are concerned that organizations or people could track them through their devices.[9] These are not abstract fears. A third of the survey respondents said "they experienced at least one type of breach or scam in the past year, and 16 percent fell victim to two or more kinds."[10]

In the United States, as the Committee knows well, we have sector-specific data security and privacy laws at the federal level but no uniform national standard that applies to all Americans and establishes a baseline for protecting all types of data. Perhaps that helps to explain why, according to a 2019 Pew Research study, 72 percent of "Americans report feeling that all, almost all or most of what they do online or while using their cellphone is being tracked by advertisers, technology firms or other companies."[11] It surely is part of the reason why 75 percent of Americans are not confident that the government will hold a company accountable if it misuses or compromises their data.[12] According to Pew's updated research in 2023, the concerns

---

[7] Müge Fazlioglu, *Privacy and Consumer Trust*, IAPP, Mar. 2023, https://iapp.org/media/pdf/resource_center/privacy_and_consumer_trust_report_summary.pdf.

[8] *Corporate data responsibility: Bridging the consumer trust gap*, KPMG, 2023, https://kpmg.com/us/en/articles/2023/bridging-the-trust-chasm.html.

[9] Jana Arbanas et al., *Data privacy and security worries are on the rise, while trust is down | 2023 Connected consumer survey*, Deloitte, 2023, https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey.html#explore.

[10] *Id.*

[11] Brooke Auxier, Lee Rainie et al., *Americas and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* at p. 6, Pew Research, Nov. 15 2019, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf.

[12] Brooke Auxier, Lee Rainie et al. *Americas and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information* at p. 9, Pew Research, Nov. 15 2019, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf.

have only grown worse. Last year, 67 percent of Americans reported that "they understand little to nothing about what companies are doing with their personal data."[13]

All of this concern about data security and privacy is negatively impacting consumer trust in AI technology and leading AI companies. According to a Cisco survey, 62 percent of global consumers are concerned about the business use of AI today, and 60 percent say that the use of AI by organizations so far has already eroded their trust.[14] American consumers are no exception to the global trend. When surveyed last year, 70 percent of Americans who have heard about AI have little to no trust in companies to make responsible decisions about how they use it in their products.[15]

Another statistic demonstrates the loss of agency that Americans feel over their data and illustrates why data minimization and other data security measures are so important in restoring Americans' trust in their government's ability to require responsible data stewardship. Although 78 percent of Americans trust themselves to make "the right decisions about their personal information," a majority doubt that anything they do will make much of a difference. Only about one in five Americans are confident that those who have their personal information will treat it responsibly.[16]

These studies are just a small sampling of consumer research that reveals deep-seated concerns—both globally and in the United States—about privacy, data use, and trust in AI companies. But Americans are also clear about the solutions to this problem, with 72 percent of Americans wanting more regulation of companies' data practices.[17] Notably, this support is bipartisan, with 68 percent of Republicans and 78 percent of Democrats expressing this view.[18] And most Americans are also clear that the specific path forward involves data minimization and other data security protections. Research consistently shows that Americans are concerned about how much data companies collect from them.

---

[13] Colleen McClain, Michelle Faverio et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research, Oct. 18, 2023, https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[14] *Generation Privacy: Young Consumers Leading the Way | Cisco 2023 Consumer Privacy Survey*, Cisco, Oct. 18, 2023, https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html

[15] Colleen McClain, Michelle Faverio et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research, Oct. 18, 2023, https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

[16] *Id.*

[17] *Id.*

[18] *Id.*

Interestingly, some studies suggest that company leaders understand the trust deficit among their consumers and broadly agree on the path forward. A 2023 KPMG survey of 250 business leaders found that 70 percent said their company increased data collection over the previous year.[19] One out of three business leaders surveyed said that consumers should be concerned about how *their* company uses personal data. Tracking consumer sentiment, 62 percent of leaders said their company should do more to protect their consumers' personal data.[20]

III. Strong Federal Data Minimization Rules Could Fix the Broken Notice and Consent Privacy Paradigm in the United States

A strong federal data minimization regime would respond to consumer concerns and finally replace the broken notice and consent approach that has defined American data security and privacy governance for decades. The "notice and consent" approach requires private entities to notify individuals and ask for their permission before collecting and utilizing their personal data.[21] These notices often take the form of privacy policies. But it would take people *hundreds* of hours to read all the privacy policies for websites and applications that most of us encounter in just a year.[22] In 2019, one in five Americans said they often or always read privacy policies,[23] and even that figure seems surprisingly high. In 2023, a majority of Americans responded to this unfair burden on consumers by just clicking "agree" without reading privacy policies.[24] This isn't

---

[19] *Corporate data responsibility: Bridging the consumer trust gap*, KPMG, 2023, https://kpmg.com/us/en/articles/2023/bridging-the-trust-chasm.html.
[20] *Id*.
[21] Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, New America's Open Technology Institute, Mar. 23, 2020, https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/ ("Notice and consent is too weak in practice to meaningfully shield individual privacy. Instead, we need comprehensive privacy legislation that will empower individuals with explicit user rights over their data, and provide strict limits on how private entities handle that data.").
[22] Geoffrey A. Fowler, *I Tried to Read All My App Policies. It Was 1 Million Words*, Washington Post, May 31, 2022, https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/; Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568, https://kb.osu.edu/server/api/core/bitstreams/a9510be5-b51e-526d-aea3-8e9636bc00cd/content.
[23] Brooke Auxier, Lee Rainie et al. *Americas and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research, Nov. 15 2019, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/
[24] Michelle Faverio, *Key findings about Americans and data privacy*, Pew Research, Oct. 18, 2023, https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

meaningful notice, it isn't meaningful consent, and it is not clear that either is achievable in the course of most of our online activities.[25] Enter data minimization, which shifts the responsibility onto companies to exercise restraint by collecting and using data only that they need to provide their products or services.

Right now, the U.S. legislative regime for data security is fragmented in ways that make consumers more vulnerable and require companies to develop complicated compliance programs in the absence of clear national rules of the road. In broad terms, a credible federal data minimization standard would require that companies only collect and process data that is reasonably necessary for the products and services that they offer, in addition to fulfilling other permissible purposes like data security and protection against fraud. A federal data privacy and security law would make clear that the obligation to minimize data applies to all aspects of the data life cycle: data collection, use, transfer, and retention. Congress has made progress in this respect, most recently in the discussion draft of the American Privacy Rights Act (APRA), which would establish a data minimization regime and robust data security requirements.

We at the Open Technology Institute believe in the power of digital technology to produce transformative innovation that serves the public interest. However, the costs of continuing to operate without a reasonable federal standard on data minimization—to American consumers, American companies, and the health of our economy—are simply too high. The proposed solution—a comprehensive federal privacy law rooted in data minimization and data security obligations—would not overburden industry. Data minimization is not a rigid concept that by itself would stifle innovation or hamstring companies, whether large or small, incumbent or start-up. Properly applied, data minimization can reduce security concerns, protect user data, and lead to better products and services.

Data minimization is not a new concept that is difficult to incorporate in federal law. Minimization and other well-established data protection principles stem from an earlier era of U.S. leadership on responsible data governance. The U.S. Department of

---

[25] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013) https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications; David Medine and Gayatri Murthy, *Companies, not people, should bear the burden of protecting data*, David Medine and Gayatri Murthy, Brookings, Dec. 18, 2019, https://www.brookings.edu/articles/companies-not-people-should-bear-the-burden-of-protecting-data/.

Health, Education, and Welfare, in 1973, published a landmark report that established a set of five Fair Information Practices (FIPs).[26] Those five principles have been further developed into principles like the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, which include the core requirements of data minimization. Those requirements, in turn, have been incorporated into legislation around the world, including Europe's General Data Protection Regulation (GDPR), Brazil's General Personal Data Protection Law (LGPD), and India's Digital Personal Data Protection Act (DPDPA).[27] Each of these laws takes a slightly different approach to minimization, but they all adopt the principle as a legal requirement. Against this global backdrop, a comprehensive U.S. federal law on data protection and privacy is conspicuously absent.

Data minimization is also widely understood by companies as a principle of risk management, but the application across companies and sectors is inconsistent. Federal codification of data minimization rules would not be seen as a novel regulatory requirement. Major U.S. tech companies, for example, already include data minimization in their privacy and data governance frameworks.[28]

IV. Strong Federal Data Security Standards Are Essential to Addressing Variations across Sectors and Data Types

OTI focuses considerably on data minimization because it is often an underappreciated aspect of securing data and protecting consumers, but there are also other basic best practices in data security that should be required as a baseline across all sectors of the economy. Strong federal legislative requirements could require companies and other organizations to do the following:

---

[26] U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[27] Using the OECD Privacy Guidelines as an illustration, the following principles collectively fall under the broader umbrella of data minimization: collection limitation, purpose specification, and use limitation. *See OECD Privacy Guidelines* (last amended Oct. 2013), Organisation for Economic Cooperation and Development, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

[28] See, *e.g.*, Meta, *Privacy Progress Update (Privacy Review)*, https://about.meta.com/privacy-progress/#how-we-do-it (listing data minimization as a core privacy principle); Google, *Your privacy is protected by responsible data practices*, https://safety.google/privacy/data/ (noting that data minimization "limit[s] the personal information that is used and saved); Google, *Our Privacy Principles*, https://safety.google/principles/ (listing as the fourth principle "We reduce the data we use to further protect your privacy.").

- **Securely store and process data.** When feasible, given the intended uses of the data, it is a best practice to encrypt data at rest (stored data) and data in transit (data being transmitted between devices and servers).
- **Apply strong access controls, which can be implemented through technical controls and administrative rules.** It is critical to ensure that only the people who need to be able to access data actually can access it.
- **Use strong methods for authentication and identity management**. Companies must ensure that data access is accompanied by robust authentication requirements, which include but are not limited to using appropriately strong passwords in combination with multi-factor authentication. Unfortunately, many data breaches take place because weak or default passwords enable the success of password-guessing efforts.[29]
- **Retain only data that is still needed by periodically reviewing data sets for relevance and deleting what is no longer needed**. As discussed in Sections I-III, minimizing the amount of available data is an important safeguard against misuse and mitigates the harms from data breaches.
- **Standardize privacy-enhancing technologies.** Advancements in encryption and increasingly secure computing environments have led to a new generation of data processing tools. Technologies like multi-party computation and zero-knowledge proofs allow for data to be processed in a way that all the data remains encrypted and no private information is disclosed. These and other privacy-enhancing technologies should become the standard for processing data.
- **Routinely assess and mitigate against data security vulnerabilities at the device, network, and application levels.** Companies should not only regularly apply updates and security patches for their hardware and software, but they

[29] Verizon Business, *2024 Data Breach Investigations Report* p. 43-44, https://www.verizon.com/business/resources/T990/reports/2024-dbir-data-breach-investigations-report.pdf; *State of Security 2024: The Race to Harness AI*, Splunk, https://www.splunk.com/en_us/form/state-of-security.html (" "...attackers often use older vulnerabilities, default passwords, and other low hanging fruit to target organizations, so a commitment to cyber hygiene is more important than ever." ").

should also be aware of and implement other common security practices, like network segmentation.[30]

There is, of course, no such thing as perfect security in either the digital or physical worlds. But common-sense best practices like these should be standard requirements in federal law, so long as they are applied with enough flexibility to account for variation in organizations' size and capacity to develop sophisticated data security programs.

Conclusion

Americans want strong and consistent protections for their data. They realize that their data can represent the most sensitive aspects of their lives. Data protection *is* consumer protection, and this committee is deeply aware of the need for companies to serve as responsible stewards of data—personal or otherwise.

Rapid advances in artificial intelligence serve as a reminder that now is the time to ensure a strong, common national standard for data security and privacy. We appreciate the Committee's bipartisan leadership on privacy and data security legislation. OTI looks forward to working with Members of Congress to help advance strong privacy and data security protections into law.

[30] See, *e.g.*, *What is Network Segmentation?*, Cisco, https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html#~how-segmentation-works.