April 7th, 2025

Dear Chairman Guthrie, Vice Chairman Joyce, and members of the Data Privacy Working Group:

Public Knowledge is encouraged by continued efforts to develop a federal privacy law. However, any forthcoming federal privacy law should build upon the work already accomplished in the drafts of the *American Data Privacy Protection Act* (ADPPA) and the *American Privacy Rights Act* (APRA), rather than relying on weaker state laws[1] (and without preempting stronger ones). These bipartisan drafts represent a robust and comprehensive approach to consumer privacy that balances the need for consumer protection with the practical realities of a global digital economy. By starting from these frameworks, Congress can craft privacy legislation that is effective at fostering consumer trust, while enabling innovation.

The ADPPA and APRA drafts were the result of extensive deliberation and input from diverse stakeholders, including lawmakers, privacy advocates, businesses, and consumers. Together, they represent a thoughtful, carefully balanced approach to key privacy concerns such as data minimization, transparency, consumer consent, and enforcement mechanisms. Both drafts incorporate key principles that address the current gaps in privacy protection, offering clear, enforceable rights for consumers, including the right to access, correct, and delete their personal data, as well as the right to opt out of certain forms of data processing. Moreover, these drafts prioritize vulnerable populations, by establishing heightened protections for children's data and other sensitive information. While neither draft was perfect[2], discarding the extensive work led by Reps. McMorris-Rodgers and Pallone would not only be harmful to the American public, but would further delay the enactment of Federal privacy legislation. As Rep. Guthrie said in his statement when announcing the Data Privacy Working Group, "the need for comprehensive data privacy is greater than ever."[3]

Public Knowledge would like to use this request for information to discuss four important topics. First, we strongly support a data minimization framework, rather than a notice and consent framework, as the foundation of any federal privacy law. Second, if a definition of "sensitive data" is included, it should align with the definition used in the *Protecting Americans Data from Foreign Adversaries Act* (PADFAA). Also, the Federal Communication Commission's privacy authority should be preserved to ensure the safety and confidentiality of our communications networks. Finally, any privacy law can only work if our federal regulators, like the FTC, are

---

[1] Aliza Vigderman, 47 States Have Weak or Nonexistent Consumer Data Privacy Laws, Security.org (Sept. 24, 2024), https://www.security.org/resources/digital-privacy-legislation-by-state/.
[2] Will McBride, Public Knowledge Opposes Weak Privacy Bill, Public Knowledge (June 26, 2024), https://publicknowledge.org/public-knowledge-opposes-weak-privacy-bill/.
[3] House Committee on Energy and Commerce, Chairman Guthrie and Vice Chairman Joyce Announce Creation of Privacy Working Group, Energy & Commerce Comm. (Feb. 12, 2025), https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-announce-creation-of-privacy-working-group.

robustly staffed, and Commissioners are given sufficient independence to pursue violators without fear or favor.

Data Minimization rather than Notice and Consent

A national privacy law should not be rooted in the flawed notice-and-consent framework, which has proven ineffective in protecting consumers. Instead, it should prioritize principles like data minimization, as outlined in the *American Data Privacy Protection Act* (ADPPA) and the *American Privacy Rights Act* (APRA). These frameworks focus on limiting the collection, use, and retention of consumer data to what is strictly necessary for specific purposes. By grounding privacy law in data minimization, we can better protect individuals from the risks of excessive commercial surveillance and ensure that businesses are held accountable for their data practices.

The current notice-and- consent system assumes that consumers can easily read and understand lengthy privacy policies, and can therefore make informed decisions about whether to share their data. However, this assumption is fundamentally flawed. Studies show that most users do not read privacy policies – not because they do not care about privacy, but because companies deliberately use complex and opaque language that makes it difficult to understand what is actually being consented to.[4] Even if consumers manage to read and understand the policies, many allow the provider to change terms at will. Moreover, consumers are often left with little real choice. In today's digital environment, many services are so ubiquitous that opting out isn't a meaningful option for most people. Users are essentially forced to accept terms if they wish to use essential services, creating a situation where consent is more of a formality than a meaningful decision. Finally, as 23 And Me's bankruptcy demonstrates, even if a company decides to "compete on privacy" by committing to strong protections, the company may still reveal the information as the result of a bankruptcy, acquisition or data breach.[5]

Further, relying on notice-and-consent as a cornerstone of privacy law fails to address the issue of over-collection of data. Companies are allowed to collect vast amounts of data with minimal restrictions, often under the guise of "informed consent." However, this data is frequently used in ways that consumers did not anticipate or understand. In contrast, data minimization ensures that companies only collect the data they truly need for the specific purpose at hand. This principle is not only more aligned with privacy protection, but it also helps to limit the opportunities for misuse or abuse of personal information.

Another critical reason to move away from notice-and-consent and toward data minimization is the increasing complexity of the technologies used to collect and process personal data. Devices like smart speakers, wearable tech, and connected home appliances often collect data passively, without users' knowledge or opportunity to consent. This makes it impossible to rely

---

[4]Joel R. Reidenberg et al., Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding, 30 Berkeley Tech. L.J. 39 (2015)

[5] John Naughton, Genetic Data Is Another Asset to Be Exploited – Beware Who Has Yours, The Guardian (Apr. 5, 2025), https://www.theguardian.com/science/2025/apr/05/genetic-data-breach-23andme-bankruptcy.

on traditional consent models. In these cases, limiting the amount of data collected - through data minimization - is a more effective way to protect privacy.

Additionally, the power imbalance between consumers and corporations further complicates the notice-and-consent approach. Once a consumer purchases a smart device or subscribes to a service, they are often locked in to any future company changes (which they reserve the right to do under their terms of service.) For example, is it fair to tell consumers that have purchased expensive devices and subscriptions that, to avoid having their personal conversations collected to train generative AI, they must throw away their previous speaker and device purchases, cancel their subscriptions and hope they can find an alternative that does not do the same? Was the consumer expected to predict both the birth of large language models trained on human speech ***and*** that the device manufacturer or service provider would unilaterally change its terms of service to collect personal conversations for this new purpose?

Even without consumer lock-in, companies control how and when privacy policies are presented to consumers, and they have the ability to design consent mechanisms that favor their own interests. For example, businesses can bury important data use disclosures in long, confusing privacy policies, making it difficult for users to make an informed choice.[6] And, as already noted, they can reserve the right to change their terms.

Data minimization, on the other hand, ensures that companies only collect what is necessary, removing users' complex decisions about data sharing in the first place. Principles like data minimization are already successfully integrated into privacy frameworks such as the ADPPA and APRA. By focusing on limiting data collection, these frameworks address the root cause of many privacy concerns—excessive data collection and misuse—without placing the burden on consumers to constantly manage their consent.

In contrast, when privacy law is based on notice-and-consent, consumers are left navigating a maze of privacy policies and consent forms, without the power to truly control their data. A national privacy law rooted in data minimization would provide clearer guidelines for companies, focusing on reducing the amount of personal information collected and ensuring that data is used only for specific, legitimate purposes. This would not only simplify compliance for businesses but also enhance consumer protection by minimizing the risks of data misuse.

For these reasons, a national privacy law should prioritize data minimization over notice-and-consent. This approach would reduce the amount of unnecessary data collected, limit the potential for exploitation, and provide stronger, more meaningful protections for consumers in the digital age. By focusing on what data is collected and for what purpose, rather than asking consumers to navigate a complex system of consent, we can create a privacy regime that is both practical and effective.

Sensitive Data Definition

---

[6]Johnathan Yerby & Ian Vaughn, Deliberately Confusing Language in Terms of Service and Privacy Policy Agreements, 23 Issues in Info. Sys. 138 (2022), https://iacis.org/iis/2022/2_iis_2022_138-149.pdf.

The definition of "sensitive data"[7] in the *Protecting Americans Data from Foreign Adversaries Act* (PADFAA) offers a comprehensive and nuanced framework that should serve as the foundation for any forthcoming privacy legislation. This definition is particularly valuable because it addresses the most vulnerable categories of personal data, including financial information, health records, biometric data, and geolocation data, all of which are especially susceptible to misuse. These types of data, when exposed or improperly accessed, can lead to serious consequences for individuals, such as identity theft, discrimination, and other privacy violations. By recognizing these data types as sensitive, PADFAA ensures that privacy protections focus on the data that poses the greatest risks to individuals' privacy and security.

Data sensitivity extends beyond protecting what we currently know; it must also account for emerging risks posed by evolving technologies. The PADFAA's definition is broad enough to encompass new forms of sensitive data, such as information from smart devices, AI systems, and even genetic data. This flexibility ensures that privacy protections remain relevant and effective as new technologies and data types continue to emerge. In this way, the definition offers the adaptability needed to keep pace with the constantly evolving digital economy, avoiding the need for frequent legislative updates to address new privacy challenges.

Incorporating PADFAA's definition into future privacy legislation also provides much-needed clarity for both regulators and businesses. A well-established definition of sensitive data enables regulators to more effectively monitor and enforce privacy protections, while providing companies with clear guidelines on how they should handle sensitive data. This clarity helps prevent confusion and ensures that companies understand their obligations, making it easier for consumers to trust that their personal information is being handled responsibly and securely.

Additionally, by limiting how and why sensitive data can be collected, processed, and shared, PADFAA's definition helps curb the exploitation of personal data. In an age of pervasive commercial surveillance and data monetization, this framework serves as a safeguard against companies profiting off sensitive data without proper regard for consumer privacy. It ensures that consumer rights are respected, particularly in an era where data collection practices are often opaque and manipulative.

FCC Privacy

The Federal Communications Commission (FCC) has been instrumental in protecting consumer privacy in the telecommunications sector for almost a century.[8] Its authority, rooted in laws like

---

[7]Protecting Americans' Data from Foreign Adversaries Act of 2024, H.R. 815, 118th Cong. § 2(11) (2023), https://www.congress.gov/bill/118th-congress/house-bill/815/text.

[8] The FCC is descended from the Federal Radio Commission, created by the Federal Radio Act of 1927. In 1934, Congress transferred authority for telecommunications common carriers such as the telephone and telegraph from the Interstate Commerce Commission to the Federal Radio Commission to create the Federal Commmunications Commission. Privacy protections for private communications were part of the predecessor acts as well as being an original provision of the Communications Act of 1934. *See generally* https://publicknowledge.org/the-proposed-privacy-bill-would-treat-your-phone-data-like-your-amazon-account-this-is-not-a-good-thing/

the Cable Privacy Act of 1984[9], and Section 222 of the Communications Act,[10] has established a robust framework for safeguarding the privacy of telephone communications. The FCC's expertise and regulatory tools, such as the ability to issue fines and enforce swift action, make it uniquely qualified to protect privacy in this complex industry.

Section 222, which governs Customer Proprietary Network Information (CPNI), not only ensures consumer privacy but also promotes competition by allowing consumers to transfer their data to rival service providers when requested. This prevents incumbent companies from using customer information to block competition and fosters a fair marketplace, benefiting consumers.

Shifting telecom privacy oversight away from the FCC risks undermining both privacy protections and competition. Without the FCC's authority, consumers would face delays of up to 90 days for data requests, compared to the FCC's current rule requiring quick turnaround and requiring providers to honor porting requests to competitors. Additionally, the ease with which consumers can switch providers could be obstructed, as telecom companies might introduce barriers to hinder competition. Furthermore, the FCC has adapted its rules to keep pace with technological advancements, such as Voice over Internet Protocol (VoIP) services and mobile phones, ensuring that privacy protections remain relevant.

Some have argued that these responsibilities could be taken over by a regulator like the FTC. While the FTC is an effective general regulator, it lacks the specialized knowledge and enforcement power needed for the telecommunications industry. This is not just Public Knowledge's opinion, but the opinion of the FTC as well.[11] The FTC cannot replicate the FCC's targeted authority to protect consumer privacy within telecom.

The FCC's role in safeguarding telecommunications privacy is vital for both protecting consumers' data and promoting competition. Shifting this responsibility would weaken privacy protections and hinder competition. To maintain a fair, transparent, and competitive telecom market, the FCC's authority must remain intact.

Enforcement

The biggest hurdle to passing a comprehensive privacy bill thus far has been due to fights about how preemptive a federal law should be, and if that law should allow for private suits. Public Knowledge has always been in favor of minimal preemption paired with robust private enforcement mechanisms.[12] However, if a federal privacy law were to preempt state laws and remove the ability for private individuals to sue, the FTC and state attorneys general would be

---

[9] Codified at 47 U.S.C. § 551.
[10] Added by the Telecommunications Act of 1996. Codified at 47 U.S.C. § 222.
[11] Lina M. Khan, Remarks of Chair Lina M. Khan Regarding the 6(b) Study on the Privacy Practices of Six Major Internet Service Providers, Fed. Trade Comm'n (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597790/20211021_isp_privacy_6b_statement_of_chair_khan_final.pdf.
[12] Harold Feld, Principles for Privacy Legislation: Putting People Back in Control of Their Information, Public Knowledge (Dec. 2017), https://publicknowledge.org/wp-content/uploads/2021/11/Feld_Paper_Formatted.pdf.

left with the sole responsibility of enforcing the law. In such a scenario, it is crucial that the FTC operates at full strength, with a fully staffed[13], bipartisan[14] commission and the necessary resources to effectively oversee the law's implementation. Without a fully functioning agency, the FTC would lack the capacity to adequately investigate violations, issue enforcement actions, and ensure that businesses comply with the law. The absence of state-level protections and private lawsuits would leave consumers vulnerable, especially without robust federal enforcement.

For the law to truly protect privacy, the FTC must be equipped with the expertise, authority, and staffing to hold companies accountable, deter violations, and ensure that privacy standards are upheld nationwide. Public Knowledge asks that before any drafting of a new privacy law begins, the Working Group publicly asks the administration not only for the reinstatement of fired FTC staffers, but the reinstatement of the illegally dismissed Democratic Commissioners. A privacy law without robust enforcement is worse than having no privacy law at all.

Conclusion

As the work begins on drafting another federal privacy bill, we hope the Working Group will preserve the data minimization framework seen in ADPPA and APRA, align any definition of sensitive data with the PADFAA, preserve the FCC's privacy authority to protect communications networks, and ensure robust federal level enforcement.

Thank you,

Sara Collins

Director of Government Affairs

Public Knowledge

[13]Alexandra Kelley & Frank Konkel, FTC Removes Around a Dozen Staff, Nextgov/FCW (Mar. 4, 2025), https://www.nextgov.com/people/2025/03/ftc-removes-around-dozen-staff/403476/.
[14] Policy Alert: Firing Democratic FTC Commissioners, The Conference Board (Mar. 19, 2025), https://www.conference-board.org/research/CED-Newsletters-Alerts/firing-democratic-ftc-commissioners.