Senators Schumer, Heinrich, Rounds, and Young - thank you for inviting me to participate in this Insight Forum on privacy and liability.

My name is Chris Lewis, and I am the President and CEO of Public Knowledge.[1] Public Knowledge is a non-profit organization that promotes freedom of expression, an open internet, and access to affordable communications tools and creative works. We know that AI has the potential to transform society for the better; but that can only happen if an appropriate regulatory framework is in place.

The first step of that framework should be to enact a comprehensive federal privacy law. This idea is not revolutionary. In the recent AI Executive Order,[2] The Administration makes clear that privacy legislation is necessary to protect all Americans and to ensure that innovation in AI is responsibly done. Everyone from think tanks[3] to trade associations[4] have made this point over the last three months. Senator Schumer, you have made this exact call yourself, along with many of your colleagues.[5]

Luckily, Congress does not need to start from scratch here. The House of Representatives, under Reps. McMorris Rodgers and Pallones leadership have created a bipartisan proposal that would minimize the amount of personal data collected, would give people rights over their data, encourage competition, and integrate important civil rights protections.

---

[1] Thank you to my Public Knowledge colleagues Sara Collins, John Bergmayer, Harold Feld, and L'Allegro Smith for their contributions to this testimony.
[2] Fact sheet: President Biden issues executive order on safe, secure, and trustworthy artificial intelligence, The White House (2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.
[3] Alex Engler et al., How privacy legislation can help address AI Brookings (2023), https://www.brookings.edu/articles/how-privacy-legislation-can-help-address-ai/.
[4] Steven Ward & Brandon Pugh, What does AI need? A comprehensive federal data privacy and security law (2023), https://iapp.org/news/a/what-does-ai-need-a-comprehensive-federal-data-privacy-and-security-law/.
[5] Gopal Ratnam, Data Privacy Law seen as needed precursor to AI Regulation Roll Call (2023), https://rollcall.com/2023/09/26/data-privacy-law-seen-as-needed-precursor-to-ai-regulation/ (last visited Nov 4, 2023)(discusses Sens. Hickenlooper, Cantwell, and Schumer's support for a federal privacy law, as well as Reps. McMorris Rodgers and Pallone).

Data minimization, as seen in Section 101 of the American Data Privacy and Protection Act, provides a strong incentive for all companies, including those developing AI systems, to only use personal data that is necessary for their specific needs. This benefits both businesses and consumers. By having clear guidelines on collection, sale, and transfer of data businesses can have certainty on whether the data they have can be used for building or training AI models. Also, personal data that is not collected is less likely to be present in data breaches.[6] Consumers get the benefit of not having to wade through complicated privacy policies, manage tedious consent menus, or try to ascertain if their personal data has been bought and sold a multitude of times. It correctly shifts the burden of data protection back onto the company that has collected and used the data.[7]

Data rights serve as a critical counterpart to the requirements of data minimization. These rights empower people to gain insights into the extent of the commercial surveillance. When individuals can access, correct, and even delete their data, they are given the ability to be proactive with their data. In the context of AI, data deletion is an especially powerful tool. If a company was never supposed to collect a person's data in the first place, giving an individual the right to request its deletion not only makes the individual whole, but discourages companies' from over collecting data in the first place. Data deletion as a right is already present in the European Union's General Data Protection Regulation, and EU citizens can request for their data to be deleted from AI systems[8]. The ADPPA also includes strong user data rights, like the right to access, correct, and delete their personal information. There is no reason for Americans to have less protections than citizens of the EU.

A well-crafted comprehensive data privacy law, like the ADPPA, would also encourage more competition in AI. Right now the largest tech companies have a monopoly not only on computational resources[9], but personal data. The current AI boom is primarily powered by commercial data surveillance, which has resulted in a small group of companies establishing

---

[6] All about CHATGPT's first data breach, and how it happened, Pluralsight (2023), https://www.pluralsight.com/blog/security-professional/chatgpt-data-breach.
[7] Mark MacCarthy et al.,Companies, not people, should bear the burden of protecting data Brookings (2022), https://www.brookings.edu/articles/companies-not-people-should-bear-the-burden-of-protecting-data/.
[8] Natasha Lomas, How to ask openai for your personal data to be deleted or not used to train its AIS TechCrunch(2023), https://techcrunch.com/2023/05/02/chatgpt-delete-data/.
[9] Jai Vipra & Sara Myers West, Computational power and ai AI Now Institute (2023), https://ainowinstitute.org/publication/policy/compute-and-ai.

dominance over the digital world.[10] While start-ups generally rely on third-party intermediaries for data, the largest tech companies exploit their control over the first-party data collection environment. They leverage the network effects generated by their vast scale, allowing them to collect and use data within platforms entirely under their ownership and control. This process has created a self-reinforcing feedback loop, progressively cementing these firms' dominance to the point where it's nearly impossible to avoid using their systems at some point during the AI development process. While not a cure-all for competition among dominant digital platforms, a data privacy law is an important part of the process of breaking up these firms' immense power. Public Knowledge has consistently supported broader antitrust and competition policy proposals to increase big tech competition that would also mitigate the power of big data collected in AI systems, including regulations promoting interoperability and preventing anticompetitive discrimination and self-preferencing.

The Administration's Blueprint for an AI Bill of Rights[11] listed both protecting privacy and preventing algorithmic discrimination as essential for making AI systems "work for the American people." We believe that an effective privacy law necessarily contains civil rights protections. The ADPPA does just that. In a letter to Reps. Pallone and McMorris Rodgers, the Leadership Conference on Civil and Human Rights called ADPPA "the best opportunity to finally provide a strong law to protect Americans' privacy and civil rights."[12] This is because the ADPPA makes clear that traditional civil rights protections apply to new technologies and explicitly prohibits algorithmic bias. The law also requires that companies perform impact assessments and audit their systems for impermissible bias. These four provisions work together to provide both a legal and technical framework to prevent these systems from continuing past practices of discrimination.

As you can see, passing a strong comprehensive privacy law like the ADPPA, would provide significant benefits to the American people, as well as encourage responsible and competitive AI innovation.

---

[10] Meredith Whittaker, *The steep cost of capture*, 28 Interactions 50–55 (2021).
[11] Blueprint for an AI bill of rights, The White House (2023), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[12] Letter to House Energy and Commerce Committee on the American Data Privacy and Protection Act, The Leadership Conference on Civil and Human Rights, https://civilrights.org/resource/letter-to-house-energy-and-commerce-committee-on-the-american-data-privacy-and-protection-act/.

While we have chosen to focus most of our testimony on privacy, we know that this particular Insight Forum is also interested in questions of who bears responsibility when these systems cause harm. We do not have a comprehensive proposal at this time, but we do have some suggestions for how to craft a liability regime.

First, we should look to the harm to see if there is an existing liability regime that applies. In April of this year, multiple agencies led by the Federal Trade Commission (FTC) released a joint public statement pledging to enforce existing rules and protections around civil rights, fair competition, consumer protection, and equal opportunity despite the use of AI tools.[13] Public Knowledge supports their strong statement. AI is found in so many systems and products that we should avoid creating "AI policy" where existing policy is sufficient. Public Knowledge applies this same approach to our application of copyright enforcement and our analysis that Section 230 of the Communications Act does not provide intermediary liability protection for generative AI creations.[14][15] Copyright law is an excellent example where decades of judicial precedent has established a balance of liability and exceptions that can be applied to emerging technologies like AI. Policymakers should avoid changes to intellectual property laws that disproportionately benefit a handful of major rights holders, curb creativity, and may have widespread detrimental consequences.

Second, end users cannot and should not be responsible for structural or endemic harms caused by these systems. Obviously individuals can use these AI tools maliciously or negligently, and should bear responsibility for those actions, including generative AI content published negligently. However, given the opacity of AI, end users will only sometimes be in a position to mitigate harms. Therefore, liability should rest with the developers of, and platforms deploying, these AI. In some instances they are the only ones who have access to the underlying model, training data, and any audits or evaluations performed to test the precision, accuracy, and risks of a given system. This places the developers and deployers in the best position to detect and mitigate any harm that could arise. Determining whether a developer of an underlying model bears responsibility versus a deployer using that model for a specific task

[13] John Newman & Amy Ritchie & Simon Fondrie-Teitler and Amritha Jayanti, FTC chair Khan and officials from DOJ, CFPB and EEOC release joint statement on ai Federal Trade Commission (2023), https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-chair-khan-officials-doj-cfpb-eeoc-release-joint-statement-ai.
[14] Nicholas Garcia & Meredith Rose, USCO AI and copyright comments Public Knowledge (2023), https://publicknowledge.org/policy/usco-ai-and-copyright-comments/.
[15] John Bergmayer, Sorry Sydney: Generative AI doesn't (and shouldn't) have a liability shield Public Knowledge(2023), https://publicknowledge.org/sorry-sydney/.

will likely be fact specific, however Congress should provide guidelines to the judiciary when making these determinations.

Third and finally, any regulation of AI will only be as effective as the government's sustained ability to understand and enforce it. This means that any body tasked with oversight and enforcement must be given sufficient resources, staff, and expertise to carry out its mission. Public Knowledge has long supported the creation of an expert regulatory agency for digital platforms.[16] Such an agency can and should include expertise and authority over algorithmic decision making, AI systems, and the digital platforms that incorporate them. A digital regulator would be nimble and keep up with the pace of innovation. A digital regulator could use its expertise to support cross-government understanding of the development of AI as other agencies apply their existing authority to the use of AI systems. It could support auditing regimes, access to data for researchers, and maintain up-to-date best practices. A digital regulator could also develop liability safe harbors for AI systems, when appropriate.

Thank you for including Public Knowledge in this important conversation. We hope to continue this dialogue as you begin to craft legislation.

[16] Harold Feld, *The Case for the Digital Platform Act: Breakups Starfish Problems and Tech Regulation* (Roosevelt Institute: New York City 2019) https://www.digitalplatformact.com/.