PREPARED WRITTEN TESTIMONY AND STATEMENT FOR THE RECORD

OF

Ryan Calo,
Lane Powell and D. Wayne Gittinger Professor of Law,
University of Washington

HEARING ON

"The Need to Protect Americans' Privacy and the AI Accelerant"

BEFORE THE

U.S. Senate Committee on Commerce, Science, & Transportation

July 11, 2024
Russell Senate Office Building
Washington, D.C.

Chairwoman Cantwell, Ranking Member Cruz, and Members of the Committee, thank you for the opportunity to share my research and views on the important issue of artificial intelligence (AI) and privacy.

I am the Lane Powell and D. Wayne Gittinger Professor of Law at the University of Washington where I hold appointments at the Information School and, by courtesy, the Paul G. Allen School of Computer Science and Engineering. I have written dozens of articles on AI, privacy, and their interaction. Together with colleagues, I founded the interdisciplinary Tech Policy Lab and Center for an Informed Public. I am a board member of the R Street Institute and serve as a privacy judge for the World Bank. I occasionally advise companies on technology policy and ethics and am of counsel to the law firm Wade, Kilpela, & Slade LLP. Prior to academia, I worked as a privacy law associate in the D.C. office of Covington & Burling LLP. The views I express in this testimony are my own.

Americans are not receiving the privacy protections they demand or deserve. Chicago resident Mike Seay did not receive the privacy protections his family deserves when, in 2014, OfficeMax sent him a marketing letter addressed to "Mike Seay, Daughter Killed in a Car Crash."[1] Facebook users did not get the privacy protections they deserve when Cambridge Analytica tricked them into revealing personal details of 87 million people through a poorly vetted Facebook app.[2] And General Motors consumers did not get the privacy protections they deserve when their driving habits were sold to insurance companies without consent, sometimes leading to higher premiums.[3]

Privacy rules are long overdue. But the acceleration of AI over the past few years threatens to turn a bad situation into a dire one.

AI exacerbates consumer privacy concerns in at least three ways. First, AI fuels an insatiable demand for consumer data. Second, AI allows companies and governments to derive intimate details about people from widely available information. And third, AI renders consumers more vulnerable to commercial exploitation by deepening the asymmetries of information and power between consumers and companies that consumer protection law exists to address. American society can no longer afford to sacrifice consumer privacy on the altar of innovation, nor leave the task of protecting Americans' privacy to a handful of individual states.

---

[1] Nesita Kwan, OfficeMax Sends Letter to "Daughter Killed in Car Crash," NBC News (January 19, 2014), online at https://www.nbcchicago.com/news/national-international/officemax-sends-letter-to-daughter-killed-in-car-crash/1986493/.

[2] Deepa Seetharaman & Katherine Bindley, Facebook Controversy: What to Know about Cambridge Analytica and Your Data, Wall Street Journal (March 23, 2018), online at https://www.wsj.com/articles/facebook-scandal-what-to-know-about-cambridge-analytica-and-your-data-1521806400.

[3] Kashmir Hill, Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies, New York Times (March 11, 2024), online at https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html.

AI fuels an insatiable demand for consumer data. AI is best understood as a set of techniques aimed at approximating some aspect of human or animal cognition using machines.[4] As I told Wired Magazine in a 2021 story about the dangers of facial recognition technology, AI is like Soylent Green: it's made out of people.[5] AI as deployed today requires an *immense* amount of data by and about people to train its models. Sources of data include what is available online, which incentivizes companies to scour and scrape every corner of the internet,[6] as well as the company's own internal data, which incentivizes them to collect as much data on consumers as possible and store it indefinitely. AI's insatiable appetite for data alone exacerbates the American consumer privacy crisis.

AI is increasingly able to derive the intimate from the available. Many AI techniques boil down to recognizing patterns in large data sets. Even so-called generative AI works by guessing the next word, pixel, or sound in order to produce new text, art, or music. Companies are increasingly able to use this capability to derive sensitive insights about individual consumers from public or seemingly innocuous information. The famous detective Sherlock Holmes—with the power to deduce whodunit by observing a string of facts most people would overlook as irrelevant—is the stuff of literary fiction. But companies *really can* determine who is pregnant based on subtle changes to their shopping habits, as Target did in 2012,[7] or diagnose postpartum depression with 83 percent accuracy based on parent Twitter activity.[8]

The ability of AI to derive sensitive information such as pregnancy or mental health based on seemingly non-sensitive information creates a serious gap in privacy protection. Many laws draw a distinction between personal and non-personal, public and private, sensitive and non-sensitive data—protecting the former but not the latter. AI breaks down this distinction, leaving everyone more vulnerable. "Contemporary information privacy protections do not grapple with the way that machine learning facilitates an *inference economy*" writes law professor Alicia Solow-Niederman "in which organizations use available data collected from individuals to generate further information about both those individuals and about other people."[9]

---

[4] Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 UC Davis Law Review 399 (2017).

[5] Tom Simonite, A Startup Will Nix Algorithms Built on Ill-Gotten Facial Data, Wired (January 12, 2021), online at https://www.wired.com/story/startup-nix-algorithms-ill-gotten-facial-data/.

[6] Daniel J. Solove & Woodrow Hartzog, The Great Scrape: The Clash Between Scraping and Privacy, online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4884485.

[7] Charles Duhigg, How Companies Learn Your Secrets, New York Times (February 16, 2012), online at https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html The rising threat to sexual privacy seems especially acute, as Danielle Keats Citron presciently argues. Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (WW Norton 2023).

[8] Munmun De Choudhury, Scott Counts, & Eric Horvitz, Predicting Postpartum Changes in Emotion and Behavior via Social Media, CHI 2013, online at https://www.microsoft.com/en-us/research/publication/predicting-postpartum-changes-emotion-behavior-via-social-media/.

[9] Alicia Solow-Niederman, Information Privacy and the Inference Economy, 117 Northwestern University Law Review 357 (2022).

AI deepens the asymmetries of power between consumers and companies that consumer protection law exists to address. Most of us think of accomplishing tasks *with* technology, such as a calculator or cash register. Increasingly, however, Americans work, play, and purchase *through* technology. The American consumer is mediated by computer code, and a mediated consumer is a vulnerable one. Our market choices—what we see, choose, and click—are scripted and arranged in advance. As I and other privacy scholars show through a series of law review articles, modern companies study and design every aspect of their interactions with consumers.[10] Companies employ people with letters after their names to study how to extract as much money and attention as possible from the user. They then design their online store, mobile game, or social media platform accordingly. Companies have an incentive to use what they know about people plus the power of design to extract social surplus from everyone else. And they do.

Sometimes the design choices of companies are so egregious that the Federal Trade Commission has pursued them as deceptive (aka "dark") patterns. A recent FTC complaint alleges, for instance, that Amazon tricked consumers into enrolling in Amazon Prime through the manipulation of defaults.[11] Such tactics are especially problematic when they combine a general understanding of consumer psychology with specific knowledge about individual consumer vulnerabilities. For example, the ridesharing platform Uber once studied whether people might be more willing to pay for surge pricing if the battery on their phone was running out.[12]

AI dials the extractive potential of "informational capitalism"[13] up to 11. Companies use AI to derive orders of magnitude more knowledge about consumers, building it into our experiences in real-time. Rather than everything costing $9.99 because it feels farther than a cent away from $10, everything will cost *the most the consumer is willing to pay* in the moment—what economists call our "reservation price."[14] Luke Stark and Jevan Hutson use the term "physiognomic AI" to refer to the practice of using machine learning to infer identities, social status, and future social outcomes based on the physical, emotional, or behavioral characteristics of consumers.[15] Such techniques are also being deployed in a variety of contexts, including "optimizing" worker productivity, teaching and learning, and on- and offline marketing.

---

[10] E.g., Ryan Calo, Digital Market Manipulation, 82 George Washington Law Review 995 (2014).

[11] FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel, Federal Trade Commission (June 21, 2013), online at https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their.

[12] Ryan Calo & Alex Rosenblat, The Taking Economy: Uber, Information, and Power, 117 Columbia Law Review 1623 (2017).

[13] Julie Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford University Press 2019).

[14] For examples, see Albert Fox Cahn, AI is quietly being used to pick your pocket, Business Insider (June 9, 2024), online at https://www.businessinsider.com/ai-quietly-picking-your-pocket-with-personalized-pricing-2024-7.

[15] Luke Stark and Jevan Hutson, Physiognomic Artificial Intelligence, 32 Fordham Intellectual Property Media and Entertainment Law Journal 922 (2022).

The future of AI is more concerning still. The increasing ability of AI to mimic people, for example, generates myriad new opportunities for consumer harm.[16] As study after study shows, people are hardwired to react to anthropomorphic technology like AI as though it is really social.[17] Thousands of people are turning to AI-powered "therapists," creating a record of their most intimate thoughts and behaviors with few privacy safeguards.[18] Companies such as Replika—the "AI companion who cares"—have even sought to monetize this human tendency to anthropomorphize by charging consumers more to enter into romantic relationships with the company's bots.[19] The AI *literally flirts with consumers* to try to get them to switch to premium.[20]

Ultimately the purpose of privacy and other consumer protection law is to offset such aggregations of corporate power. As Professor Robert Lande shows through a detailed analysis of the legislative records of the Sherman Act, the FTC Act, and other turn of the century consumer protection laws, "Congress was concerned principally with preventing 'unfair' transfers of wealth from consumers to firms with market power."[21] This is why Section V of the FTC Act instructs the Commission to pursue "unfair" and deceptive practice. Substitute the term "AI" for "market power" and Congress' responsibility is clear: consumers need their government to help offset the immense asymmetries of information and power that AI provides the companies who deploy it.

Federal consumer privacy legislation is long overdue. The question is not whether America should have rules governing privacy. The question is why we still do not. Few believe that the internet, social media, or AI are ideal as configured. Industry's relentless pursuit of consumer data has undermined privacy, fueled misinformation,[22] and is harming the environment.[23] Existing safeguards are deeply inadequate.[24]

---

[16] Ian Kerr, Bots, Babes and the Californication of Commerce, 1 University of Ottawa Law and Technology Journal 285 (2004); Woodrow Hartzog, Unfair and Deceptive Robots, 74 Maryland Law Review 786 (2015).

[17] Ryan Calo, Robotics and the Lessons of Cyberlaw, 103 California Law Review 513 (2015).

[18] Simon Coghlan, Kobi Leins, Susie Sheldrick, Marc Cheong, Piers Gooding, Simon D'Alfosno, To chat or not to chat: Ethical Issues with using chatbots in mental health, Digit Health (June 22, 2023), online at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10291862/.

[19] Daniella DiPoala & Ryan Calo, Socio-Digital Vulnerability, online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4686874.

[20] Id. The example comes from Boine, Claire. 2023. "Emotional Attachment to AI Companions and European Law." MIT Case Studies in Social and Ethical Responsibilities of Computing, no. Winter 2023 (February). https://doi.org/10.21428/2c646de5.db67ec7f.

[21] Robert H. Lande, Wealth Transfer as the Original and Primary Concern of Antitrust: The Efficiency Interpretation Challenged, 34 Hastings Law Journal 65 (1982).

[22] Renée DiResta, The Supply of Disinformation Will Soon Be Infinite, The Atlantic (September 20, 2020), online at https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400/.

[23] Clare Duffy, Google's greenhouse gas emissions are soaring thanks to AI, CNN (July 3, 2024), online at https://www.cnn.com/2024/07/03/tech/google-ai-greenhouse-gas-emissions-environmental-impact/index.html.

There is a lingering concern that privacy rules will hamper innovation. The opposite is true. Today's absence of privacy rules is actively undermining consumer trust.[25] Just as spam threatened to make email unusable until Congress passed the CAN-SPAM Act, so has the unfettered collection, processing, use, and sharing of data led to a crisis of consumer confidence. Recent research by Pew suggests that an astonishing *eighty-one percent* of Americans assume AI companies will use their information in ways with which they are not comfortable.[26] Meanwhile the EU, among our largest trading partners, refuses to certify America as "adequate" on privacy and does not allow consumer data to flow freely between our economies. What is the point of American innovation if no one trusts our inventions?

Individual states such as Illinois, California, and Washington have responded to consumer harms and mistrust by passing privacy rules of their own.[27] Congress can and should look to such laws as a model. Yet it would be unwise to leave privacy legislation entirely to the states. The internet, social media, and AI are global phenomena; they do not respect state borders. Regulating a distributed industry is quintessentially the province of the federal government (and the reason for the Commerce Clause in the Constitution). Expecting tech companies to comply with a patchwork of laws depending on what state a consumer happens to access their services is unrealistic and wasteful. And the prospect that some states will pass privacy rules is small comfort to the millions upon millions of Americans who reside in states that have not.

Congress should pass comprehensive privacy legislation that protects American consumers, reassures our trading partners, and gives clear, achievable guidelines to industry. Data minimization rules—which obligate companies to limit the data they collected and maintain about consumers—could help address AI's insatiable appetites. Broader definitions of covered data could clarify that inferring sensitive information about consumers carries the same obligations as collecting it. And rules again data misuse or abuse could help address consumer vulnerability in the face of growing asymmetry. Congress has the power to deliver innovation Americans and the world can start to trust.

Congress should also look toward the future. Passing comprehensive privacy legislation is necessary today. But technology will not stand still. My parting recommendation is for Congress to start to prepare now for the next wave of innovation. In particular, Congress should reestablish the Office of Technology Assessment (OTA). For twenty years, the OTA helped Congress anticipate and understand emerging technologies and make wiser decisions around them. Hearings are important, but there is

---

[24] Ari Ezra Waldman, Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power (Cambridge University Press 2021).

[25] Neil Richards, Why Privacy Matters (Oxford University Press 2021).

[26] Colleen McClain, Michelle Faverio, Monica Anderson, & Eugene Park, How Americans View Data Privacy, Pew Research Center (October 18, 2023), online at https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

[27] The Illinois Biometric Information Privacy Act of 2008; the California Privacy Protection Act of 2018, as amended by the California Privacy Rights Act; the Washington My Health Data Act of 2023.

no substitute for a dedicated, interdisciplinary, bipartisan staff. Congress should also adequately fund other expert bodies—especially the National Institute of Standards and Technology. Only by ensuring that Congress has access to deep and impartial technical expertise can America hope to anticipate future disruption.

Thank you for this opportunity to testify before the Committee. I look forward to a robust discussion.