S. HRG. 118–732

THE NEED TO PROTECT AMERICANS' PRIVACY AND THE AI ACCELERANT

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

JULY 11, 2024

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
61–871 PDF WASHINGTON : 2025

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MARIA CANTWELL, Washington, *Chair*

AMY KLOBUCHAR, Minnesota	TED CRUZ, Texas, *Ranking*
BRIAN SCHATZ, Hawaii	JOHN THUNE, South Dakota
EDWARD MARKEY, Massachusetts	ROGER WICKER, Mississippi
GARY PETERS, Michigan	DEB FISCHER, Nebraska
TAMMY BALDWIN, Wisconsin	JERRY MORAN, Kansas
TAMMY DUCKWORTH, Illinois	DAN SULLIVAN, Alaska
JON TESTER, Montana	MARSHA BLACKBURN, Tennessee
KYRSTEN SINEMA, Arizona	TODD YOUNG, Indiana
JACKY ROSEN, Nevada	TED BUDD, North Carolina
BEN RAY LUJÁN, New Mexico	ERIC SCHMITT, Missouri
JOHN HICKENLOOPER, Colorado	J. D. VANCE, Ohio
RAPHAEL WARNOCK, Georgia	SHELLEY MOORE CAPITO, West Virginia
PETER WELCH, Vermont	CYNTHIA LUMMIS, Wyoming

LILA HARPER HELMS, *Staff Director*
MELISSA PORTER, *Deputy Staff Director*
JONATHAN HALE, *General Counsel*
BRAD GRANTZ, *Republican Staff Director*
NICOLE CHRISTUS, *Republican Deputy Staff Director*
LIAM MCKENNA, *General Counsel*

CONTENTS

WITNESSES

APPENDIX

THE NEED TO PROTECT AMERICANS' PRIVACY AND THE AI ACCELERANT

THURSDAY, JULY 11, 2024

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:04 a.m., in room SR–253, Russell Senate Office Building, Hon. Maria Cantwell, Chair of the Committee, presiding.

Present: Senators Cantwell [presiding], Klobuchar, Peters, Tester, Rosen, Luján, Hickenlooper, Welch, Cruz, Thune, Wicker, Fischer, Moran, Sullivan, Blackburn, Budd, Schmitt, and Vance.

OPENING STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

The CHAIR. Good morning. The Senate Committee on Commerce, Science, and Transportation will come to order.

I want to thank the witnesses for being here today for testimony on the need to protect Americans' privacy and AI as an accelerant to the urgency of passing such legislation.

I want to welcome Dr. Ryan Calo, University of Washington School of Law and Co-Director of the University of Washington Technology Lab; Ms. Amba Kak, Co-Executive Director of the AI Now Institute in New York; Mr. Udbhav Tiwari, Director, Global Product Policy for Mozilla, San Francisco; and Mr. Morgan Reed, President of ACT | The App Association of Washington, D.C.

So thank you all for being here for this very, very important hearing. We are here today to talk about the need to protect Americans' privacy and why AI is an accelerant that meets the needs of us passing legislation soon.

Americans' privacy is under attack. We are being surveilled.

[Feedback in the hearing room.]

The CHAIR. Wow, I am being tracked.

[Laughter.]

The CHAIR. We are being surveilled, tracked online in the real world through connected devices and now when you add AI it is like putting fuel on a campfire in the middle of a windstorm.

For example, a Seattle man's car insurance increased by 21 percent because his Chevy Volt was collecting detailed information about his driving habits and sharing it with data brokers who then shared it with his insurance company. The man never knew the car was collecting the data.

Data about our military members including contact information and health conditions is already available for sale by data brokers

for as little as $.12. Researchers at Duke University were able to buy such datasets for thousands of our active military personnel.

Every year Americans make millions of calls, texts, chats to crisis lines seeking help when they are in mental distress. You would expect this information would be kept confidential but a nonprofit suicide crisis line was sharing data from those conversations with its for-profit affiliates that it was using to train its AI product.

Just this year the FTC sued a mobile app developer for tracking consumers' precise location through software it embedded in the grocery list and shopping rewards app. The company used this data to sort consumers into precise audience segments. Consumers whose use of this app helped them remember when to buy peanut butter did not expect to be profiled and categorized into a precise audience segment like, quote, "parents of preschoolers."

These privacy abuses and millions of others that are happening every day are bad enough but now AI is an accelerant and they are the reason why we need to help in speeding up our privacy law.

AI is built on data, lots of it. Tech companies cannot get enough to train their AI models, your shopping habits, your favorite videos, who your kids' friends are, all of that, and we are going to hear testimony today from Professor Calo about this issue, about how AI gives the capacity to derive sensitive insights about individuals.

So it is not just the data that is being collected. It is the ability to have sensitive insights about individuals into the system. This, as some people have said—you are referring to your testimony now—is creating an inference economy that could become very challenging.

That is why I think you also point out, Dr. Calo, that a privacy law helps offset the power of these corporations and why we need to act. I also want to thank Ms. Kak for her testimony because she is clearly talking about that same corporate power and the unfair and deceptive practices which we have already given to the FTC as their main authority.

But the lack of transparency about what is going on with prompts and the AI synergy is that people are no longer just taking personal data and sending us cookie ads.

They are taking that and putting it actually into prompt information. This is a very challenging situation and I think your question is, are we going to allow our personal data to train AI models is a very important question for our hearing today.

We know that they want this data to feed their AI models to make the most amount of money. These incentives are really a race to the bottom where most privacy protected companies are at a competitive disadvantage.

Researchers project that if current trends continue companies training large language models may run out of new publicly available high-quality data to train AI systems as early as 2026.

So without a strong privacy law when the public data runs out, nothing stopping it from using our private data, I am very concerned that the ability of AI to collect vast amounts of personal data about individuals and create inferences about them quickly at very low cost can be used in harmful ways like charging consumers different prices for the same product.

I talked to a young developer in my state. I said, what is going on, and he said, well, I know one country is using AI to basically give it to their businesses. I said, well, why would they do that?

Well, because they want to know when a person calls up for a reservation at a restaurant how much income they really have. If they do not really have enough money to buy a bottle of wine they are giving the reservation to someone else.

So the notion is that discriminatory practices can already exist with just a little amount of data for consumers. AI in the wrong hands is also, though, a weapon. Deep fake phone scams are already plaguing my state. Scammers used AI to clone voices to defraud consumers by posing as a loved one in need of money.

These systems can recreate a person's voice in just minutes, taking the familiar grandparent scam and putting it on steroids. More alarming, earlier this month the Director of National Intelligence reported that Russian influence actors are planning to covertly use social media to subvert our elections.

The ODNI called AI, quote, "A maligned influence accelerant," end quote, saying that it was being used to more convincingly tailor video and other content ahead of the November election.

Just two days ago, the Department of Justice reported that it dismantled a Russian bot farm intended to sow discord in the United States using AI Russian-created scores of fictitious user profiles on X being generated, post, and then use those bots to repost "like" comments on the post, further amplifying the original fake posts.

So this was possible at tremendous scale, given AI. I am not saying that misinformation might have not existed before and may not have been placed in a chat group but now with the use of bots and AI accelerant that information can be more broadly disseminated very, very quickly.

So privacy is not a partisan issue. According to the Pew Research, a majority of Americans across the political spectrum want more support for regulation. I believe our most important private data should not be bought or sold without our approval and tech companies should serve the—and make sure that they implement these laws and help stop this kind of interference.

The legislation that Representative McMorris Rodgers and I have worked on I think does just that and I want to say I very much appreciate this morning legislation that Senator Blackburn and I will be introducing called the COPIED Act, which provide much needed transparency around AI-generated content.

The COPIED Act will also put creators including local journalists, artists, and musicians back in control of their content with a watermark process that I think is very much needed.

I will now turn to the Ranking Member Senator Cruz for his opening statement.

STATEMENT OF HON. TED CRUZ,
U.S. SENATOR FROM TEXAS

Senator CRUZ. Thank you, Madam Chair.

American prosperity depends upon entrepreneurs. These are ambitious and optimistic men and women who are willing to take risks, pursue their dreams, and try to change the world.

They mortgage their own homes. They put everything on the line to build a business that fills an unmet need or does something better than what is offered today.

But throughout history prosperity and human flourishing has been stymied or delayed by governments that impose regulatory policies to address supposed harms but in actuality overstated risk in order to protect incumbent operators, often large and powerful companies that did not want to compete and that just happened to give big campaign checks to the politicians in power.

The United States has mostly chosen a different path, one where a free enterprise system governed by the rule of law allows Americans to freely pursue their ideas, grow their own businesses, and compete without having to obtain permission from all-knowing bureaucrats.

Today's hearing on data privacy and artificial intelligence is a debate about which regulatory path we will take.

Do we embrace our proven history, one with entrepreneurial freedom and technological innovation, or will we adopt the European model where government technocrats get to second guess and manage perceived risks with economic activity, ultimately creating an environment where only big tech with its armies of lawyers and lobbyists exist.

Consider this. In 1993 at the dawn of the tech age the economies of the United States and the European Union were, roughly, equal in size.

Today the American economy is nearly 50 percent larger than the EU's. The tech boom happened in America in part because Congress and the Clinton administration deliberately took a hands-off approach to the nascent internet.

The result was millions of jobs and a much higher standard of living for Americans. Unfortunately, the Biden administration and many of my colleagues are suggesting the European model for AI, based heavily on hysterical doomsday prophecies to justify a command and control Federal regulatory scheme that will cause the United States to lose our technological edge over China.

The Biden administration's AI executive actions as well as many of the AI legislative proposals call for a new regulatory order that protects giant incumbent operators and discourages innovation with supposedly optional best practices or guidance written by all-knowing bureaucrats, some of whom were recently employed by the same big tech firms they seek to regulate and some of whom hope to be employed again by those same big tech firms right after they write the rules that benefit those giant big tech firms.

We already see Federal AI regulators and Biden allies talking about the need to stop, quote, "bias," quote, "misinformation," quote, "discrimination" in AI systems and algorithms. That is code for speech police. If they do not like what you say they want to silence it.

Now, AI can certainly be used for nefarious purposes just like any other technology, but to address specific harms or issues we should craft appropriate and targeted responses.

For example, Senator Klobuchar and I have introduced the bipartisan Take It Down Act which targets bad actors who use AI to create and publish fake lifelike explicit images of real people.

Our bill, which is sponsored by many Republican and Democrat members of this committee, would also require big tech to follow a notice and take down process so ordinary Americans who are victimized by these disturbing images can get them offline immediately.

The bipartisan Take It Down Act is a tailored solution to a real problem. On behalf of the teenage girls and others who have been victimized by deep fake explicit imagery I hope that this committee will take up soon the Take It Down Act and pass it and move it to the floor and get it signed into law.

As I conclude, I would like to address a related matter, the American Privacy Rights Act—APRA. I support Congress—not the FTC or any Federal agency but Congress setting a nationwide data privacy standard.

Not only is it good for Americans to be empowered with privacy protections, but it is good for American businesses that desperately need legal certainty given the increasingly complex patchwork of state laws.

But our goal should not be to pass any uniform privacy standard but rather the right standard that protects privacy without preventing U.S. technological innovation.

I have discussed APRA with Chairwoman McMorris Rodgers and will continue my offer to work with her but right now this bill is not the solution. It delegates far too much power to unelected commissioners at the FTC.

It focuses on algorithmic regulations under the guise of civil rights which would directly empower the DEI speech police efforts underway at the Biden White House, harming the free speech rights of all Americans.

As currently constructed APRA is more about Federal regulatory control of the Internet than personal privacy. In the end, it is the giant companies with vast resources that ultimately benefit from bills like APRA at the expense of small businesses.

The path that Congress needs to take is to put individuals in control of the privacy of their own data and give them transparency to make decisions in the marketplace, and I look forward to working with my colleagues to do exactly that.

The CHAIR. Thank you, Senator Cruz.

We will now turn to our panel starting with Dr. Calo. Thank you so much. We are really proud of the work that the University of Washington has done. I think we are on both.

Senator Cruz is mentioning the innovation economy. I think we have that down in the Northwest, but we also want to make sure we have down the important protections that go along with it.

So thank you, Dr. Calo, for your presence.

STATEMENT OF RYAN CALO, LANE POWELL AND D. WAYNE GITTINGER PROFESSOR OF LAW, UNIVERSITY OF WASHINGTON

Mr. CALO. Chair Cantwell, Ranking Member Cruz, and members of the Committee, thank you for the opportunity to share my research and views on this important topic.

I am a law professor and information scientist at the University of Washington where I co-founded the Tech Policy Lab and Center

for an Informed Public. The views I express today are entirely my own.

Americans are not receiving——

The CHAIR. Dr. Calo, could you just bring that microphone a little closer to you?

Mr. CALO. Of course.

The CHAIR. Thank you.

Mr. CALO. Americans are not receiving the privacy protections they demand or deserve, not when Cambridge Analytica tricked them into revealing personal details of 87 million people through a poorly vetted Facebook app, not when car companies share their driving habits with insurance companies without their consent, sometimes leading to higher premiums as the senator mentioned.

Privacy rules are long overdue but the acceleration of artificial intelligence in recent 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. Sources of data include what is available online which incentivizes companies to scour and scrape every corner of the internet, as well as the company's own internal data which incentivizes them to collect as much data as possible and store it indefinitely. AI's insatiable appetite for data alone deeply exacerbates the American consumer privacy crisis.

Second, AI is increasingly able to derive the intimate from the available. Many AI techniques boil down to recognizing patterns in large datasets. Even so-called generative AI works by guessing the next word, pixel, or sound in order to produce new text, art, or music.

Companies increasingly leverage this capability of AI to derive sensitive insights about individual consumers from 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 reportedly did in 2012.

And, finally, AI deepens the asymmetries of information and power between consumers and companies that consumer protection law exists to arrest.

The American consumer is a mediated consumer. We increasingly work, play, and shop through digital technology, and a mediated consumer is a vulnerable one. Our market choices, what we see, choose, and click are increasingly scripted and arranged in advance.

Companies have an incentive to use what they know about individual and collective psychology plus the power of design to extract as much money and attention as they can from everyone else.

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.

A recent survey by the Pew Research Center suggests that an astonishing 81 percent of Americans assume that companies will use AI in ways for which they are not comfortable—81 percent. Just for

context, something between 30 and 40 percent of Americans identify as Taylor Swift fans.

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? More and more individual states, from California to Colorado, Texas to Washington, are passing privacy or AI laws to address their residents' concerns.

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 boundaries, and the prospect that some states will pass privacy rules is small comfort to the 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 collect 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 against data misuse could help address consumer vulnerability in the face of a growing asymmetry.

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

[The prepared statement of Mr. Calo follows:]

PREPARED STATEMENT OF RYAN CALO, LANE POWELL AND D. WAYNE GITTINGER PROFESSOR OF LAW, UNIVERSITY OF WASHINGTON

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

[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*.

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.

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]

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

---

[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.*

[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).

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.

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

---

[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).

[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.*

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]

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 e-mail 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 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.

---

[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] Renee 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.*

[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.

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

The CHAIR. Thank you, Dr. Calo.

Ms. Kak, thank you so much. Welcome. We look forward to your testimony.

STATEMENT OF AMBA KAK, CO-EXECUTIVE DIRECTOR, AI NOW INSTITUTE

Ms. KAK. Thank you, Chair Cantwell, Ranking Member Cruz, and esteemed members of this committee. Thank you for inviting me to testify.

We are at a very clear inflection point in the trajectory of AI. Without guardrails to set the rules of the road we are committing ourselves to more of the same, to carrying forward extractive, invasive, and often predatory data practices and business models that have characterized the past decade of the tech industry.

We are also committing ourselves to the seamless transition of big tech from surveillance monopolies to AI monopolies. A Federal data privacy law could break this cycle, especially one with strong data minimization, which could challenge the culture of impunity and recklessness in the AI industry that is already hurting both consumers and competition.

If there is a single point I want to make in today's testimony it is that now is the moment when passing such a law actually matters before the trajectory has been set.

Data privacy regulation is AI regulation and it provides many of the tools that we need to protect the public from harm. But let us get concrete. How might the AI market shape up differently in the presence of a strong data privacy law?

First, with data minimization rules firms would need to put reason in place of recklessness when it comes to decisions about what data to collect, the purposes to which it can be used, and for how long it can be stored.

These requirements would empower lawmakers but also the public to demand very basic accountability. So before Microsoft, for example, rushes to release its new Recall.ai feature, which, by the way, takes continuous screenshots of everything you see or do on your computer, the company might need to ask itself and, importantly, document its answer does the utility of this feature outweigh the honeypot it is creating for bad actors?

As a security researcher quickly discovered with Microsoft Recall it is actually scarily trivial for an attacker to use malware to extract a record of everything you have ever viewed on your PC.

Now, a strong data minimization mandate would have nipped this in the bud. It would have likely disincentivized the development of such a patently insecure feature to begin with.

Second, we would have transparency about the data decisions that affect us all. Meta and Google recently announced updates unilaterally, of course, to their terms which allow AI training from user data.

Now, we know about this because European users were alerted by Meta. Without a legal mandate to require it, of course, American users received no such notification and users in—of Reddit are

also similarly up in arms because their content was just sold to the highest bidder, in this case Google, for use of training its AI.

But it is important to remember that a privacy law would offer much more than just transparency in every single instant I mentioned. Purpose limitation rules would prevent big tech from using AI as its catch-all justification to use and combine data across contexts and store it forever.

The FTC has already penalized Amazon for storing the voice data of children indefinitely, using AI as its excuse. But we cannot rely on this kind of one-off enforcement. There needs to be rules of the road.

And these rules, it is important to remember, would not just safeguard our privacy. They would also act as a powerful check on the data advantages currently being consolidated by big tech to build a moat around them and stave off competition in AI.

Third, in a world with a data privacy mandate AI developers would need to make data choices that deliberately prevent discriminatory outcomes. So we should not be surprised when we see that women are seeing far less ads for high-paying jobs in Google ads. That is 100 percent a feature of data decisions that have already been made upstream.

I mean, the good news here is that these are avoidable problems, and it is not just in scope for privacy law. I would say it is integral to protecting people from the most serious abusers of this data and where specific AI practices have sort of inherent, well-established harms, emotion recognition systems that have faulty scientific foundations or pernicious forms of ad targeting. The law would hold them entirely off limits.

Finally—and here is the thing about very large-scale AI—it is not only computationally, ecologically, and data intensive it is also very, very expensive to develop and run.

Now, these eye-watering costs will need a path to profit and by every account a viable business model still does not exist. Now, it is precisely in this kind of an environment with a few incumbent firms feeling the pressure to turn a profit that predatory business models emerge.

Meanwhile, we are hearing new research that LLM systems are capable of hyper personalized inferences about us even from the most general prompts. You do not need to be a clairvoyant to see that all roads might well be leading us right back to the surveillance advertising business model that got us here.

So, to conclude, there is nothing about the current trajectory of AI that is inevitable and as a democracy the U.S. has a huge opportunity to take global leadership and shape this next era of tech so that it reflects the public interest and not just the bottom lines of very few companies.

This is the moment for action. Thank you.

[The prepared statement of Ms. Kak follows:]

PREPARED STATEMENT OF AMBA KAK, CO-EXECUTIVE DIRECTOR, AI NOW INSTITUTE ON BEHALF OF HERSELF AND DR. SARAH MYERS WEST, CO-EXECUTIVE DIRECTOR, AI NOW INSTITUTE

Chair Cantwell, Ranking Member Cruz, and esteemed Members of the Committee, thank you for inviting me to testify on this important set of issues. I deeply appreciate this Committee for taking the initiative to spotlight this urgently needed

conversation, and in particular for recognizing that privacy and AI innovation are mutually reinforcing goals that can, and must, be advanced in concert. My name is Amba Kak, and I co-lead the AI Now Institute, a leading policy research institute founded in 2016 that focuses on the social and economic impacts of artificial intelligence technologies. I have spent over fifteen years as a global policy expert designing and advocating for technology policy in the public interest, examining topics ranging from privacy to competition to algorithmic accountability, across roles in government, industry, and civil society. I recently served as a senior advisor on artificial intelligence at the Federal Trade Commission, where my role was to provide technological expertise in support of the agency's enforcement and policy work, focused on how to mitigate and redress harms from data-driven systems like AI. This testimony is offered on behalf of myself and my colleague Dr. Sarah Myers West, and our remarks are based on research we have conducted at AI Now.[1]

As excitement and trepidation about large-scale AI systems continues to fill headlines and hearings, it's important to remember that nothing about the current trajectory of these privately developed technologies is inevitable. In a democracy, the trajectory of powerful technologies should be shaped in the public interest through public deliberation, not solely by a handful of corporate actors driven, ultimately, by commercial incentives: regulation can play a crucial role in ensuring such democratic shaping of technological systems.

Which brings me to the one overarching point I want to make in today's testimony: the trajectory of AI is at a crucial inflection point. Without regulatory intervention, we are doomed to replicate the extractive, invasive, and often harmful data practices and business models that have characterized the past decade of the tech industry. A Federal data privacy law, especially one with strong data minimization, could act as a foundational intervention to break this cycle and challenge the culture of impunity and recklessness that is hurting both consumers and competition.

In fact, the notion that we need to wipe away years of regulation and policy and create new frameworks from scratch for AI serves large industry players more than it does the rest of us: it serves to delay, and to provide current actors with significant influence on the scope and direction of such policymaking. AI systems are not wholly novel. Far from it. And rather than view them that way, to responsibly govern these technologies we must instead disaggregate these systems, or the "AI stack," into their composite inputs, recognizing the details of how they work and what they require to operate. These include close examination of data, computational infrastructure, and labor. Precise and technically aware regulatory strategies can then be deployed at different layers of this stack, preventing cloud companies from using their dominant market position to restrict competition in the AI market, for example; or copyright strategies against use of artistic works by image-generation tools; or, as is the subject of this testimony, AI firms from the irresponsible collection and retention of personal information.[2] Once this is done, we can explore whether new approaches to address previously unanticipated harms or to tackle specific sectoral use cases are needed. Before that, though, we must leverage and continue to strengthen the regulatory toolbox we have already honed over the past decade.

To illuminate my argument, I will divide it into three specific points:

First, privacy risks are implicated across the AI life cycle. The generative AI boom further unleashes new forms of familiar privacy harms, supercharges the incentives for irresponsible data surveillance, and creates conditions ripe for extractive and exploitative business models.

Second, the turn toward large-scale AI further consolidates Big Tech's already staggering control over consumer data, which deepens power asymmetries and allows these companies to act recklessly and with impunity. A strong data minimization rule would ensure not only the advancement of privacy, but would also act as a powerful curb on the concentration of power we've seen in this sector.

---

[1] See generally Amba Kak and Sarah Myers West, "AI Now 2023 Landscape: Confronting Tech Power," AI Now Institute, April 11, 2023, *https://ainowinstitute.org/2023-landscape.*

[2] See Jai Vipra and Sarah Myers West, "Computational Power and AI," AI Now Institute, September 27, 2023, *https://ainowinstitute.org/publication/policy/compute-and-ai;* Tejas Narechania and Ganesh Sitaraman, "An Antimonopoly Approach to Governing Artificial Intelligence," Vanderbilt Policy Accelerator for Political Economy and Regulation, Vanderbilt University, October 6, 2023, *https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2023/10/06212048/Narechania-Sitaraman-Antimonopoly-AI-2023.10.6.pdf.pdf;* and Jennifer Cobbe, Michael Veale, and Jatinder Singh, "Understanding Accountability in Algorithmic Supply Chains," 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23), April 7, 2023, *https://ssrn.com/abstract=4430778.*

Finally, a legally binding data privacy mandate, including strong data minimization, individual data rights, algorithmic impact assessments, and protections against algorithmic discrimination, offers a foundational toolkit for demanding accountability from AI companies.

I. *Privacy risks are implicated across the AI life cycle.* The generative AI boom further unleashes new forms of familiar privacy harms, supercharges the incentives for irresponsible data surveillance, and creates conditions ripe for extractive and exploitative business models.

In the wake of a highly charged AI race with companies rushing to release new products and features to market before competitors, we're seeing a sharp uptick in privacy lapses, from unexpected leaks of personal information in chatbot outputs[3] to features that threaten to fundamentally compromise the privacy and security of our personal devices.[4] While the list of egregious and obvious privacy failures is already long, we also need a systematic approach that brings into view every stage of the AI data life cycle as well as captures the more structural pathologies set in motion by the AI boom.

In this vein, we look into privacy harms that (1) emanate at the training and development stage, (2) emanate at the application and output stage, and those that (3) emanate from the business models and incentives shaping the AI market.

(I) *Training and development stage.* AI models are trained on large amounts of data, and the early stages of training and then fine-tuning models can set in motion some of the most harmful and far-reaching data practices.

While there is a lack of basic transparency about the datasets used to train many commercially available models today, we know that at least some have taken advantage of publicly available data, scraping the web to create massive datasets of images and text, as well as voice and video data. In 2009, Meta changed its settings so that much previously private user data became public by default while users scrambled to revert to their original settings.[5] A month later, Mark Zuckerberg disingenuously argued that privacy was no longer the "social norm."[6] Statements like this subvert the most basic privacy expectations of citizens whose digital lives are hoovered up by firms for profit, shielded by broad and inscrutable terms of service and settings that can be changed without people's consent. Only through public scandals like Cambridge Analytica in 2018 did the public become aware that it had to contend with the dangers of this kind of centralized data power in the hands of a few companies.[7]

Developments in generative AI have brought into sharp focus the stakes of this free-for-all approach to mining the public sphere. Soon after the public release of ChatGPT, questions from the public about what data these AI models had been trained on began to circulate,[8] followed by panic when people began to realize that ChatGPT was sometimes leaking personal data "accidentally" in response to prompts.[9]

We're also seeing Big Tech firms store and use data collected in one context for other unanticipated purposes, using AI as a catchall justification. Companies haven't given clear answers to the question of whether or not they're using internal data to train new AI models,[10] and Meta and Google recently announced an update

---

[3] Jordan Pearson, "ChatGPT Can Reveal Personal Information from Real People, Google Researchers Show," *Vice,* November 29, 2023, *www.vice.com/en/article/88xe75/chatgpt-can-reveal-personal-information-from-real-people-google-researchers-show.*

[4] Zak Doffman, "Google Confirms Serious AI Risks for iPhone and Android Users," *Forbes,* February 15, 2024, *www.forbes.com/sites/zakdoffman/2024/02/12/google-warns-as-free-ai-upgrade-for-iphone-android-and-samsung-users.*

[5] Nick Bilton, "'He Doesn't Believe in It': Mark Zuckerberg Has Never Cared about Your Privacy, and He's Not Going to Change," *Vanity Fair,* November 20, 2018, *https://www.vanityfair.com/news/2018/11/mark-zuckerberg-has-never-cared-about-your-privacy.*

[6] Bobbie Johnson, "Privacy No Longer a Social Norm, Says Facebook Founder," *Guardian,* January 10, 2010, *https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.*

[7] Ibid.

[8] Clothilde Goujard, "Italian Privacy Regulator Bans ChatGPT," *Politico,* March 31, 2023, *https://www.politico.eu/article/italian-privacy-regulator-bans-chatgpt.*

[9] See Nicholas Carlini *et al.,* "Extracting Training Data from Large Language Models," 30th USENIX Security Symposium, December 2020, *https://arxiv.org/abs/2012.07805;* Nicholas Carlini *et al.,* "Extracting Training Data from Diffusion Models," January 2023, *https://arxiv.org/abs/2301.13188;* and OpenAI, "March 20 ChatGPT Outage: Here's What Happened," March 24, 2023, *https://openai.com/blog/march-20-chatgpt-outage.*

[10] Cordilia James, "Are Instagram and Facebook Really Using Your Posts to Train AI? What to Know," *Wall Street Journal,* June 21, 2024, *https://www.wsj.com/tech/ai/meta-ai-training-instagram-facebook-explained-a3d36cdb.*

to their terms that explicitly allows training of AI from user data.[11] These fundamental choices of what data to use to train AI models determine the likelihood of inaccurate and discriminatory outputs. Recent research demonstrates that as AI models scale, using larger and larger datasets like the ones used in current LLMs, the tendency to produce inaccurate and harmful stereotypes also scales.[12] Meanwhile, a decade of evidence on predictive AI systems now bears out the "garbage in, garbage-out" thesis, which holds that inaccurate, incomplete, and discriminatory training datasets go on to produce decisions or recommendations in high-stakes domains with harmful consequences for people's lives.[13]

(2) *Applications, outputs, and decision-making stage.* Downstream, we see a new range of privacy threats culminate as AI models are applied to consumer-facing applications, or used in systems that aid or make decisions, recommendations, or inferences that impact people's lives in material ways.

Generative AI systems currently on the market have been unexpectedly and routinely leaking personal information that is traced back to training datasets, including sensitive or even confidential data.[14] While generative AI companies advise their users not to include personal information in their prompts, many still do;[15] more concerningly, research suggests that LLM-powered systems like ChatGPT are capable of making detailed and sensitive inferences even from apparently anonymized prompts.[16] Mindful of these unresolved and persistent privacy challenges, many of the largest technology firms have banned their employees from using services like ChatGPT.

With a scramble to rush to market and a lack of regulatory friction, we're seeing multiple AI companies announce untested and potentially harmful applications of AI that rely on people's sensitive information—including biometrics—to make questionable inferences. For example, on the occasion of OpenAI's recent rollout of Sora, a chatbot that provides multimedia output in response to prompts, CEO Sam Altman claimed that the software could detect emotional states from people's voice recordings—even as there is mounting evidence (acknowledged by regulators globally[17]) that such inferences have dubious scientific validity, and potentially reinforce inaccurate and discriminatory stereotypes. Data privacy laws around the world are already being used to put in place strict limitations on specific kinds of data use that have well-known harms, including such "emotion recognition" systems[18] as well as targeted advertising to children.[19]

(3) *Business model harms.* As the past decade illuminates, tech firms already have strong incentives for irresponsible and invasive data collection, fueled primarily by a business model that relies on personalized behavioral targeting of consumers with advertising. The AI boom exacerbates this, fueling a race to the bottom. In fact, a key feature of the current market for large-scale AI is that it is not only computationally, ecologically, and data intensive, it is also very, *very* expensive to

---

[11] Eli Tan, "When the Terms of Service Change to Make Way for A.I. Training," *New York Times,* June 26, 2024, *https://www.nytimes.com/2024/06/26/technology/terms-service-ai-training.html.*

[12] Abeba Birhane et al, "On Hate Scaling Laws For Data-Swamps", June 28 2023, *https://arxiv.org/abs/2306.13141.*

[13] See Heather Rodroguez, "Garbage In, Garbage Out: The Potential Pitfalls of Artificial Intelligence," Texas A&M University College of Arts and Sciences, January 19, 2023, *artsci.tamu.edu/news/2023/01/garbage-in-garbage-out-the-potential-pitfalls-of-artificial-intelligence.html;* and Joan M. Teno, "Garbage In, Garbage Out—Words of Caution on Big Data and Machine Learning in Medical Practice," JAMA Forum, February 16, 2023, *https://jamanetwork.com/journals/jama-health-forum/fullarticle/2801776.*

[14] Lily Hay Newman, "ChatGPT Spit Out Sensitive Data When Told to Repeat 'Poem' Forever," *Wired,* December 2, 2023, *https://www.wired.com/story/chatgpt-poem-forever-security-roundup.*

[15] Heidi Mitchell, "Is It Safe to Share Personal Information With a Chatbot?" *Wall Street Journal,* January 18, 2024, *https://www.wsj.com/tech/ai/ai-chatbot-sharing-personal-information-229d41a0.*

[16] Mack DeGeurin, "ChatGPT Can 'Infer' Personal Details from Anonymous Text," *Gizmodo,* October 17, 2023, *gizmodo.com/chatgpt-llm-infers-identifying-traits-in-anonymous-text-1850934318.*

[17] Information Commissioner's Office, "'Immature Biometric Technologies Could Be Discriminating against People' Says ICO in Warning to Organisations," October 26, 2022, *https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations.*

[18] Access Now, European Digital Rights (EDRi), Bits of Freedom, Article 19, and IT-Pol, "Prohibit Emotion Recognition in the Artificial Intelligence Act," May 2022, *https://www.accessnow.org/wp-content/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf.*

[19] See the American Data Privacy and Protection Act, H.R. 8152, 117th Congress, June 21, 2022, *https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-1178152rh.pdf.*

develop and run these systems.[20] These eye-watering costs will need a path to profit. By all accounts, though, a viable business model remains elusive.[21] It is precisely in this kind of environment, with a few incumbent firms feeling the pressure to turn a profit, that predatory business models tend to emerge.

Finally, there is also a broader harm that cuts across the indiscriminate collection and retention of data at these various stages of the AI life cycle: the more data that is collected and stored indefinitely, the more we are creating "honeypots" or "goldmines for cyber criminals"[22] that are an attractive target for interception by unauthorized third parties,[23] including malicious state and non-state actors. We already have examples of the real human costs of careless retention of data, from biometric information of Afghan citizens in American-managed databases that fell into the hands of the Taliban,[24] to the intricate web of third-party data brokers that buy and sell sensitive information about people that can be used to target them unfairly or to hinder their access to credit, housing, and education.[25] Data minimization is based on the premise that information that's never collected in the first place cannot be breached; and that which is deleted after it's no longer needed is no longer at risk.

II. The turn toward large-scale AI further consolidates Big Tech's already staggering control over consumer data, which deepens power asymmetries and allows these companies to act recklessly and with impunity.

Large-scale AI depends principally on data and compute resources (this includes both cloud computing and hardware components like chips) as essential inputs. Big Tech companies are already positioned at a considerable advantage at many points in the AI stack. Currently, the largest consumer technology companies such as Google, Microsoft, and Amazon dominate access to such compute resources (and other companies, as a rule, depend on them for these resources).[26] This is closely related to these companies' pre-existing data advantage, which enables them to collect and store large amounts of good-quality data about billions of people via their vast market penetration.

The idea that "data is everywhere" and therefore not a scarce resource is intuitively appealing but misses the point: quality data *is* scarce. Datasets with high levels of human curation and human feedback; niche datasets especially in high-impact sectors like finance or healthcare; datasets that come with assurances of accuracy, legitimacy, and diversity at scale are becoming a key source of competitive advantage for Big Tech companies, especially in the hypercompetitive generative AI market. This data advantage can give models developed by Big Tech companies an edge over those developed without the benefit of such data. Indeed, access to high-quality data can result in smaller models (those trained on less data and requiring less computational power for training) that perform better than larger models trained without such quality data. OpenAI has reportedly already used YouTube data to train its models, which leaves the door open for Google to use data not only from YouTube, but also from Gmail, Google Drive, and all its other properties.[27] Similarly, Microsoft can potentially use data from its enterprise services, and AWS from

---

[20] Seth Fiegerman and Matt Day, "Why AI Is So Expensive," Bloomberg, April 30, 2024, *https://www.bloomberg.com/news/articles/2024-04-30/why-artificial-intelligence-is-so-expensive.*

[21] See David Cahn, "AI's $600B Question," Sequoia Capital, June 20, 2024, *https://www.sequoiacap.com/article/ais-600b-question;* and Benj Edwards, "So Far, AI Hasn't Been Profitable for Big Tech," *Ars Technica,* October 10, 2023, *https://arstechnica.com/information-technology/2023/10/so-far-ai-hasnt-been-profitable-for-big-tech.*

[22] Dimitri Sirota, "The Art Of Letting Go: How Data Minimization Can Improve Cybersecurity And Reduce Cost," *Forbes,* March 29, 2023, *https://www.forbes.com/sites/forbestechcouncil/2023/03/29/the-art-of-letting-go-how-data-minimization-can-improve-cybersecurity-and-reduce-cost/?sh=641958c75340.*

[23] For examples of "leaky" data from Internet of things (IoT) devices and mobile phones, leaving personal information of users vulnerable to interception, see Anna Maria Mandalari *et al.,* "Blocking without Breaking: Identification and Mitigation of Non-Essential IoT Traffic," Proceedings of Privacy Enhancing Technologies Symposium (PETS), May 11, 2021, *https://doi.org/10.48550/arXiv.2105.05162.*

[24] Eileen Guo and Hikmat Noori, "This Is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban," *MIT Technology Review,* August 30, 2021, *https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points.*

[25] See, for example, Federal Trade Commission, "FTC Sues Kochava for Selling Data That Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations," August 29, 2022, *https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.*

[26] Jai Vipra and Sarah Myers West, "Computational Power and AI," AI Now Institute, September 27, 2023, *https://ainowinstitute.org/publication/policy/compute-and-ai.*

[27] Jon Victor, "Why YouTube Could Give Google an Edge in AI," *The Information,* June 14, 2023, *https://www.theinformation.com/articles/why-youtube-could-give-google-an-edge-in-ai.*

its cloud services. Each of these companies has also forged partnerships and acquisitions in specific sectors that give them access to troves of sensitive data, such as in the electronic health records space.[28]

Repositories of publicly available data currently available online are also likely to dwindle or become less valuable soon in comparison to proprietary datasets held by these companies. We're already seeing a trend toward more restrictions on publicly available data[29] expensive content deals between large AI firms and big publishers like *The Atlantic* and *Axel Springer*[30] and websites like *Reddit* and *Stack Overflow;*[31] and a general lack of transparency around what datasets are being used to train AI.[32]

In this environment, unlike other actors that must largely rely on third-party intermediaries to access data, large firms are exploiting the fact that they directly control the vast majority of the environment in which data is collected; they are able to take advantage of the network effects associated with the scale at which they operate by collecting, analyzing, and using data within platforms they wholly own and control.[33] This is a product of a self-reinforcing feedback loop, which over time has led to these firms being so dominant and pervasive that it is virtually impossible *not* to use their systems.[34]

This market reality must inform any privacy and AI-specific regulatory efforts. Privacy and competition law are too often siloed from each other,[35] leading to interventions that could easily compromise the objectives of one issue over the other.[36] And firms are, in turn, taking advantage of this to amass information asymmetries that contribute to further concentration of their power.[37]

This concentration of power enabled by control over data isn't just a problem for potential competitors of Big Tech. Too much centralized economic power in the hands of too few harms our democracy—especially when these very same actors have proven themselves to be reckless and far from dependable custodians of this power. Amid the hype surrounding AI, companies are rushing to market with technologies that are far from ready to be broadly accessible. Google recently rolled out its AI Overviews feature in its search engine results; within days it was producing

---

[28] See Karen Weise, "Amazon to Acquire One Medical Clinics in Latest Push into Health Care," *New York Times,* July 21, 2022, *https://www.nytimes.com/2022/07/21/business/amazon-one-medical-deal.html;* Tina Reed, "Google Cloud Announces Epic Partnership," *Axios,* November 14, 2022, *https://www.axios.com/2022/11/14/google-cloud-announces-epic-partnership;* and Epic, "Epic and Microsoft Bring GPT–4 to EHRs," May 5, 2023, *https://www.epic.com/epic/post/epic-and-microsoft-bring-gpt-4-to-ehrs.*

[29] Isabelle Basquette, "AI Startups Have Tons of Cash, but Not Enough Data. That's a Problem," *Wall Street Journal,* June 15, 2023, *https://www.wsj.com/articles/ai-startups-have-tons-of-cash-but-not-enough-data-thats-a-problem-d69de120.*

[30] Damon Beres, "A Devil's Bargain with OpenAI," *Atlantic,* May 29 2024, *https://www.theatlantic.com/technology/archive/2024/05/a-devils-bargain-with-openai/678537.*

[31] Associated Press, "As AI Learns from Stack Overflow, Reddit, and More Platforms, Companies Are Adapting While Users Protest," *Fast Company,* July 3, 2024, *https://www.fastcompany.com/91150665/ai-learns-stack-overflow-reddit-facebook-adapting-users-protest.*

[32] See Mike Isaac, "Reddit Wants to Get Paid for Helping to Teach Big A.I. Systems," *New York Times,* April 18, 2023, *https://www.nytimes.com/2023/04/18/technology/reddit-ai-openai-google.html;* @XDevelopers, March 29, 2023, *https://x.com/XDevelopers/status/1641222782594990080;* and Paresh Dave, "Stack Overflow Will Charge AI Giants for Training Data," *Wired,* April 20, 2023, *https://www.wired.com/story/stack-overflow-will-charge-ai-giants-for-training-data.*

[33] Lina M. Khan, "Sources of Tech Platform Power," *Georgetown Law Technology Review* 2, no.2 (2018): 325–334, *https://georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Khan-pp-225–34.pdf;* Lina M. Khan, "The Separation of Platforms and Commerce," *Columbia Law Review* 119, no. 4 (May 2019): 973–1098, *https://columbialawreview.org/content/the-separation-of-platforms-and-commerce.*

[34] Kashmir Hill, "I Tried to Live without the Tech Giants. It Was Impossible," *New York Times,* July 31, 2020, *https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html.*

[35] Udbhav Tiwari, "Competition Should Not Be Weaponized to Hobble Privacy Protections on the Open Web," Mozilla (blog), April 12, 2022, *https://blog.mozilla.org/netpolicy/2022/04/12/competition-should-not-be-weaponized-to-hobble-privacy-protections-on-the-open-web.*

[36] Maurice E. Stucke, "The Relationship between Privacy and Antitrust," *Notre Dame Law Review Reflection* 97, no. 5 (2022): 400–417, *https://ndlawreview.org/wp-content/uploads/2022/07/Stucke_97-Notre-Dame-L.-Rev.-Reflection-400-C.pdf.*

[37] For example, Article 5 of the European Union's Digital Markets Act prohibits large "gatekeeper" platforms from the cross-use of personal data between its various service offerings, without explicit user consent. See European Commission, "The Digital Markets Act: Ensuring Fair and Open Digital Markets," accessed July 9, 2024, *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.*

inaccurate, nonsensical, and even dangerous answers to people's queries.[38] Meta's new AI agents, which the company integrated into millions of Instagram and Facebook accounts, have generated misinformation and misled people into believing they were interacting with real human beings.[39] And Microsoft has been broadly panned for proposing a new AI-enabled feature named Recall that raises numerous privacy-related red flags.

These are the very same companies that resist regulatory guardrails in the name of "innovation." It's time to question the premise: Is this scramble for reckless growth by a handful of surveillance monopolies really innovation? It's not surprising that these companies, free from regulatory constraints or competitive market pressures, are acting out. A data privacy mandate that embeds transparency and accountability around how these companies build AI, and when they determine they are fit for market release, isn't curbing innovation: it's a long overdue check on these companies.

III. Data privacy law—in particular strong data minimization, impact assessments, data rights, and protections against algorithmic discrimination—provides a foundational toolkit for demanding accountability from AI companies.

Taking stock of some of the myriad, diffused ways in which AI is poised to heighten threats to our individual and collective privacy, and worsen the concentrations of power in Big Tech, we can now ask: *How might the AI market develop differently in the presence of a strong, broad-ranging Federal privacy law?*

a. Data minimization:

Data minimization rules impose a proactive obligation on entities to put reasonable limits on the collection, use, and retention of personal data in the interest of the individual and group data holders. These "data minimization" rules, which are described in recent proposals such as the APRA,[40] are a core part of global data protection laws. As AI Now, Accountable Tech, and EPIC emphasize in our "Zero Trust AI Framework," data minimization rules are essential levers at a time when AI is tipped to further exacerbate information asymmetries between individuals and communities on one hand, and the large corporations that create and collect data about them on the other.[41]

Collection limitation, for example, would force firms to adhere to limits when it comes to data surveillance and acquisition—to build within the constraints of necessity and proportionality. This would replace reckless organizational data cultures with reflexivity that forces engineers to calibrate decisions about data, keeping in mind the privacy and security vulnerabilities these create. In response to Microsoft's announcement of its Recall feature that continuously screenshots our activities on the computer, the lawmakers and the public would be empowered to demand basic accountability: is such data surveillance, that creates a honey pot for bad actors and unauthorized access, at all proportionate? It is likely, in fact, that this feature may have never been announced in the first place had the company done even a rudimentary impact assessment that evaluated risks to privacy and security. Put simply, a strong data minimization mandate would have disincentivized the development of these patently unsafe features to begin with.

A purpose limitation rule, on the other hand, could restrain Big Tech monopolies from endlessly combining data collected for distinct purposes in pursuit of consolidating their data advantage against competitors. We already have examples of these rules being applied to protect consumers from harm. The FTC has also penalized Amazon for storing children's voiceprints—highly sensitive data—and shot down the company's justification that it would be used to improve its Alexa algorithm.[42]

Most crucially, data minimization rules don't hinge on user consent: they apply regardless, overcoming the now-well-known deficiencies of a privacy regime that hinges exclusively on individuals being able to meaningfully exercise choices online given the structural power asymmetries that abound between individuals and mas-

---

[38] Ellie Stevens, "The 7 Most Shocking Google AI Answers We've Seen So Far," *Fast Company,* May 30, 2024, *https://www.fastcompany.com/91132974/shocking-google-ai-overview-answers.*

[39] "Meta's New AI Agents Confuse Facebook Users," Associated Press, April 20, 2024, *https://www.voanews.com/a/meta-s-new-ai-agents-confuse-facebook-users-/7576420.html.*

[40] U.S. Senate Committee on Commerce, Science, and Transportation, "Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation," April 7, 2024, *https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-dat a-privacy-legislation.*

[41] Accountable Tech, AI Now Institute, and EPIC, "Zero Trust AI Governance," AI Now Institute, August 10, 2023, *https://ainowinstitute.org/publication/zero-trust-ai-governance.*

[42] Federal Trade Commission, "U.S. v. Amazon.com (Alexa)," FTC Cases and Proceedings, July 21, 2023, *https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3128-amazon com-alexa-us-v.*

sive tech firms.[43] Just this week, Open AI CEO Sam Altman, in collaboration with another company, announced Thrive AI Health, pitched as a "hyper-personalized AI health coach."[44] They set out a pervasive vision of data surveillance, ranging from highly intimate sleeping, eating, and exercise behaviors combined with medical data. The premise is that because individuals can "choose" whether to share this data, any privacy concerns are put to rest. This flies in the face of a decade of evidence that indicates we cannot rely solely on people's choices to protect them, when the long-term implications of unauthorized access, out-of-context sharing, or malicious use are difficult if not impossible for the average consumer to meaningfully comprehend. This is the outcome of a regulatory environment that has failed to place limits on the unrestrained collection, storage, and use of sensitive data, allowing companies to fall back on consent as a catchall defense.

Beyond the general principle of data minimization, a data privacy law could include prohibitions on specific kinds of data use that have well-known harms, such as targeted advertising to children,[45] or uses based on sensitive data categories,[46] or the use of data about people's interior mental states in so-called "emotion recognition" systems that have been repeatedly found to be based on faulty foundations.[47] Perhaps, Open AI CEO Sam Altman would have likely been stopped in his tracks before claiming the recent multimedia chatbot Sora would be able to "detect people's emotional states" from people's voice recordings.

b. Data rights:

Data rights are a crucial complement to the proactive obligations of data minimization, as they empower individuals to ascertain the nature and scale of commercial surveillance, and to act on such information to correct, order deletion, or otherwise seek redress if they believe any other obligations owed to them under the legislation have not been fulfilled.

Currently, the only constraint on usage of any consumer data for training of proprietary models comes from the terms of service of those products, which can be changed at will, as Google and Meta recently did. Notable too that while European users were alerted by Meta that it would use publicly available posts to train its AI, American users received no such notification.[48] With a comprehensive data privacy law, these individuals would have, at minimum, the ability to demand transparency around the use of their data.

Under the latest text of APRA, consumers would also have a broad right to opt out of algorithmic decision-making that comprises "consequential decisions"—defined as decisions, including ads, that may impact an individual's equal access to housing, employment, healthcare, and so on.[49] Such algorithmic decision-making is ubiquitous today, with limited oversight. As just one example, an IBM survey in 2023 showed that out of 8,500 participants in the survey, 42 percent were already using AI screening to filter out candidates, and another 40 percent were in the process of integrating with such technology.[50] These screening softwares have been known to filter out qualified candidates based on their age, gender, or even hobbies, with marginalized candidates bearing the brunt of maximum harm.[51] A right to opt out of consequential decisions would allow these candidates a fairer review of their

---

[43] See Federal Trade Commission, "Commercial Surveillance and Data Security Rulemaking," notice, August 11, 2022, *https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking;* and David Medine and Gayatri Murthy, "Companies, Not People, Should Bear the Burden of Protecting Data," Brookings, December 18, 2019, *https://www.brookings.edu/articles/companies-not-people-should-bear-the-burden-of-protecting-data.*

[44] Sam Altman and Ariana Huffington, "AI-Driven Behavior Change Could Transform Health Care," *Time,* July 7, 2024, *https://time.com/6994739/ai-behavior-change-health-care.*

[45] See American Data Privacy and Protection Act, H.R. 8152, 117th Congress, *https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS–1178152rh.pdf.*

[46] Ibid.

[47] Access Now, European Digital Rights (EDRi), Bits of Freedom, Article 19, and IT-Pol, "Prohibit Emotion Recognition in the Artificial Intelligence Act."

[48] Eli Tan, "When the Terms of Service Change to Make Way for A.I. Training."

[49] U.S. Senate Committee on Commerce, Science, and Transportation, "Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation," April 7, 2024, *https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-dat a-privacy-legislation.*

[50] "Data Suggests Growth in Enterprise Adoption of AI is Due to 'Widespread Deployment by Early Adopters, But Barriers Keep 40 percent in the Exploration and Experimentation Phase,'" IBM Newsroom, January 10, 2024, *https://newsroom.ibm.com/2024–01–10-Data-Suggests-Growth-in-Enterprise-Adoption-of-AI-is-Due-to-Widespread-Deployment-by-Early-Adopters.*

[51] Aaron Rieke and Miranda Bogen, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias," Upturn, December 10, 2018, *https://www.upturn.org/work/help-wanted.*

applications and would force companies to put better pipelines to employment in place that do not exacerbate entrenched inequalities in the workplace.

c. Impact Assessments:

A data privacy law should also include a mandate for impact assessments or audits of AI systems in order to proactively identify and mitigate harms, including relating to discrimination, privacy, and security. These evaluations go beyond conventional privacy impact assessments that assess systems against relatively narrow privacy and security criteria, in favor of a more expansive stocktaking that requires companies to evaluate whether particular groups will be harmed as a result of the design or use of the AI system. Researchers like Dr. Alex Hanna and Dr. Mehtab Khan, for example, have put forward a multilayered framework to scrutinize the multiple complex layers of large-scale AI models.[52]

One could imagine that some of the most concerning recent AI features and products, from Microsoft's Recall to Google AI Overviews, would perhaps never have been announced or brought to market had firms been required to comprehensively evaluate the privacy and security implications of their systems before release.

A note of caution on impact assessments: while such evaluations are positive in theory, these obligations must be drafted to ensure meaningful accountability. There is a significant risk that any audit or evaluation standard can devolve into a superficial checkbox exercise,[53] more useful in offloading liability than in protecting the public. With that in mind, we recommend the following:

- Meaningful assessments that mandate evaluation should happen *before* products are made available for use in the public domain, and should be subject to evaluation on an ongoing basis while in operation. It is essential that the criteria for such evaluations not be limited to narrow technical parameters or be tested only under so-called "laboratory-like conditions."[54]
- Evaluations must be conducted by independent, disinterested, and adequately resourced and protected third parties such as researchers, civil society, or the appropriate Federal agencies, by charging that such evaluations are subject to both regulatory and public scrutiny.
- There must be real consequences for a failure to mitigate or prevent harms that are identified. This includes strict penalties but also, crucially, abandoning systems that are designed in ways that make such harms inevitable.

d. Prohibition against discrimination:

A range of privacy proposals, both in the United States and globally, include protections against using personal data in AI in ways that discriminate.[55] It is now well documented that AI systems are routinely, and often structurally, biased in ways that entrench and embed historical inequities[56] in sensitive social domains

---

[52] Mehtab Khan and Alex Hanna, "The Subjects and Stages of AI Dataset Development: A Framework for Dataset Accountability," *Ohio State Technology Law Journal,* September 13, 2022, *http://dx.doi.org/10.2139/ssrn.4217148.*

[53] See Amba Kak and Sarah Myers West, *Algorithmic Accountability: Moving Beyond Audits,* AI Now Institute, April 11, 2023, *https://ainowinstitute.org/publication/algorithmic-accountability;* and Sasha Costanza-Chock, Inioluwa Deborah Raji, and Joy Buolamwini, "Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem," FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, June 2022, *https://doi.org/10.1145/3531146.3533213.* Professor Woody Hartzog refers to audits and similar procedural interventions as "privacy half measures" that are necessary but wholly insufficient in protecting users; see *Hearing On "Oversight Of A.I.: Legislating On Artificial Intelligence" Before the Subcommittee On Privacy, Technology, And The Law,* U.S. Senate Committee On The Judiciary, September 12, 2023 (Statement of Woodrow Hartzog), *https://techpolicy.press/wp-content/uploads/2023/09/2023-09-12_pm_-_testimony_-_hartzog.pdf.*

[54] See Ben Green and Lily Hu, "The Myth in the Methodology: Towards a Recontextualization of Fairness in Machine Learning," 35th International Conference on Machine Learning, 2018, *https://econcs.seas.harvard.edu/files/econcs/files/green_icml18.pdf;* Shira Mitchell, Eric Potash, Solon Barocas, Alexander D'Amour, and Kristian Lum, "Algorithmic Fairness: Choices, Assumptions, and Definitions," *Annual Review of Statistics and Its Application* 8 (2021): 141–163, *https://doi.org/10.1146/annurev-statistics-042720–125902;* and Rodrigo Ochigame, "The Long History of Algorithmic Fairness," *Phenomenal World,* January 30, 2020, *https://www.phenomenalworld.org/analysis/long-history-algorithmic-fairness.*

[55] U.S. Senate Committee on Commerce, Science, and Transportation, "Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation."

[56] See Federal Trade Commission, "Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems," public statement, April 25, 2023, *https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/joint-statement-enforcement-efforts-against-discrimination-bias-automated-systems;* White House, "Blueprint for an AI Bill of Rights," August 2022, *https://www.whitehouse.gov/ostp/ai-bill-of-rights;* Samir Jain, "CDT and Coalition Urge White House to Ensure Forthcoming AI Executive Order Advances Civil Rights &

like healthcare,[57] hiring,[58] education,[59] housing,[60] and criminal justice.[61] This should not come as a surprise given that these systems necessarily draw their map of "the world" from data that reflects discriminatory histories and sentiments. As recently highlighted in the fact sheet accompanying the Biden administration's Blueprint for an AI Bill of Rights, several Federal agencies are already applying existing laws and mechanisms to address algorithmic discrimination in housing, employment, and other realms.[62] A civil rights provision in a Federal privacy law would provide an overarching means of redress against AI systems that perpetuate discrimination.

To conclude, the key lesson of the past decade has been understanding that control over data is about power asymmetries, and since companies derive clear commercial benefit from widening this asymmetry, regulation is essential to protect the public from harm. Passing strong Federal privacy legislation is a critical and overdue step in that direction.[63] And while it is true that the United States is already behind in terms of enacting a comprehensive data privacy law, in those countries that have these legislative mandates in place, there have been major gaps and ambiguities in implementation. An opportunity exists, therefore, to enact and creatively apply foundational privacy principles to the emergent landscape of AI systems, setting the gold standard of enforcement for the rest of the world.

The CHAIR. Thank you, Ms. Kak. Thank you for that testimony.

And I—the notion that—in your testimony you talked about how just the sound of our voice could be used to project different detections and different outcomes of what people are doing is just very disturbing. Very disturbing.

So, Mr. Tiwari. Welcome.

STATEMENT OF UDBHAV TIWARI, DIRECTOR, GLOBAL PRODUCT POLICY, MOZILLA

Mr. TIWARI. Chair Cantwell, Ranking Member Cruz, and esteemed members of the Committee, thank you for the opportunity

---

Civil Liberties," Center for Democracy & Technology, September 5, 2023, *https://cdt.org/insights/cdt-and-coalition-urge-white-house-to-ensure-forthcoming-ai-executive-order-advances-civil-rights-civil-liberties.*

[57] Ziad Obermeyer *et al.,* "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," *Science* 366 (October 25, 2019): 447–453, *https://www.science.org/doi/10.1126/science.aax2342.*

[58] See U.S. Equal Employment Opportunity Commission, "Artificial Intelligence and Algorithmic Fairness Initiative," January 23, 2023, *https://www.eeoc.gov/ai;* Pauline T. Kim, "Data-Driven Discrimination at Work," 58 *William & Mary Law Review* 857, February 1, 2017, *https://scholarship.law.wm.edu/wmlr/vol58/iss3/4;* Ifeoma Ajunwa, "Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law," 63 *St. Louis University Law Journal* 21 (2019), September 10, 2018, *https://ssrn.com/abstract=3247286;* and Aaron Rieke and Miranda Bogen, "Help Wanted."

[59] See Kristin Woelfel, Elizabeth Laird, and Maddy Dwyer, "Letter to ED and the White House from Tech Policy, Civil Rights, and Civil Liberties Advocates Calling for Civil Rights Guidance and Enforcement Regarding EdTech and AI," Center for Democracy & Technology, September 20, 2023, *https://cdt.org/insights/letter-to-ed-and-the-white-house-from-tech-policy-civil-rights-and-civil-liberties-advocates-calling-for-civil-rights-guidance-and-enforcement-regarding-edtech-and-ai;* and Andre M. Perry and Nicol Turner Lee, "AI Is Coming to Schools, and If We're Not careful, So Will Its Biases," Brookings, September 26, 2019, *https://www.brookings.edu/articles/ai-is-coming-to-schools-and-if-were-not-careful-so-will-its-biases.*

[60] See U.S. Justice Department, "Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising," press release, June 21, 2022, *https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known;* Lauren Kirchner and Matthew Goldstein, "Access Denied: Faulty Automated Background Checks Freeze Out Renters," *The Markup,* May 28, 2020, *https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renter;* Ridhi Shetty, "CDT Comments to Federal Agencies Highlight Risks of Data Used in Tenant Screening," Center for Democracy & Technology, June 2, 2023, *https://cdt.org/insights/cdt-comments-to-federal-agencies-highlight-risks-of-data-used-in-tenant-screening.*

[61] Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, "Machine Bias," *ProPublica,* May 23, 2016, *https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.*

[62] White House, "Blueprint for an AI Bill of Rights."

[63] Accountable Tech, AI Now Institute, and EPIC, "Zero Trust AI Governance."

to testify on the critical issue of protecting Americans' privacy in the age of artificial intelligence.

My name is Udbhav Tiwari and I am the director of global product policy at Mozilla. Today I will discuss the urgent need for comprehensive privacy legislation, the importance of data minimization, and the role of privacy-enhancing technologies in fostering responsible AI development.

At Mozilla we approach tech policy issues through a unique vantage point as a nonprofit foundation, an open source community, and a tech company. We build the open source Firefox web browser Mozilla VPN and products like Solo, an AI-powered website builder for micro SMBs and solopreneurs.

These products are used by hundreds of millions of people around the world and Mozilla's mission is to ensure that the Internet is a global public resource open and accessible to all.

We believe that comprehensive privacy legislation is foundational to any AI framework and that maintaining U.S. leadership in AI requires America to lead on privacy and user rights.

Privacy is a critical component of AI policy, not just because AI has the potential to accelerate privacy-related harms but because AI systems thrive on data and the drive to develop advanced AI models has also intensified the demand for vast amounts of personal information.

This data collection, often done without the adequate consent or via deceptive choices, poses significant risks to individual privacy and security.

By championing policies that promote innovation, create clear rules of the road for companies, and protect fundamental user rights, we can create both a competitive and a level playing field for the American AI industry and prepare domestic champions for global leadership.

At the core of these principles and policies should be data minimization. Data minimization is a crucial principle that ensures only the necessary data is collected and used for specific purposes. In the context of AI data minimization can be achieved through several strategies including informed consent and ensuring there is privacy by design.

While legislation is essential, technical advances must work hand in hand with legislative solutions to create a new safe and private future. In the context of what the ecosystem currently needs we need a significant investment in privacy-enhancing technologies to develop AI systems that respect and protect individual privacy.

Openness and open source are also essential ingredients for improving verifiable and meaningful privacy in AI technologies. Open approaches play a vital role in promoting innovation and preventing the concentration of power in the hands of few companies that my fellow panelists have spoken about.

They enable the economic benefit of AI to be more widely shared amongst businesses of different sizes and capabilities. This leads to increased investment and job creation.

We also have clear evidence from open source development practices that openness allows a diverse input and collaboration, fostering the development of privacy preserving techniques that can benefit everyone rather than relying on security through obscurity.

Turning to the potential risks of AI amplifying privacy violations, we know that online manipulation, targeted scams, and online surveillance are not new risks in our digital lives.

However, AI technologies can supercharge such harms, creating risks like profiling and manipulation, bias and discriminations, and deep fakes and identity misuse.

To mitigate these risks we need comprehensive Federal privacy legislation. This should be accompanied by strong regulatory oversight and continued investments in privacy-enhancing technologies.

We must also ensure that AI systems are transparent and accountable with mechanisms in place to address privacy violations and provide recourse for affected individuals underpinned by disclosure and accountability.

When it comes to the AI's potential to impact civil liberties the risk cannot be understated. The same technologies that drive innovation can also be used to infringe upon fundamental rights and be used by big tech companies to trample on individual privacy.

It is therefore imperative that AI development and deployment are guided by principles that protect civil liberties. This includes safeguarding freedom of expression, preventing unlawful surveillance, and ensuring that AI systems do not perpetuate discrimination or bias.

In conclusion, protecting Americans' privacy in the age of AI is a critical challenge that requires comprehensive legislation. As we navigate the complexities of AI and privacy it is crucial to strike a balance between innovation and protection.

Thank you for the opportunity to testify today. I look forward to your questions and to working with you to protect Americans' privacy in the AI era.

[The prepared statement of Mr. Tiwari follows:]

PREPARED STATEMENT OF UDBHAV TIWARI, DIRECTOR, GLOBAL PRODUCT POLICY, MOZILLA

Chair Cantwell, Ranking Member Cruz, and esteemed members of the Committee,

Thank you for the opportunity to testify on the critical issue of protecting Americans' privacy in the age of artificial intelligence (AI). My name is Udbhav Tiwari, and I am the Director of Global Product Policy at Mozilla. Today, I will discuss the urgent need for comprehensive privacy legislation, the importance of data minimization, and the role of privacy-enhancing technologies in fostering responsible AI development. America can continue to be a leader in AI by putting in place clear rules of the road on privacy that will help to spur beneficial competition and create a level playing field for players of all sizes instead of a race to the bottom.

About Mozilla

At Mozilla, we approach tech policy issues from a unique vantage point as a non-profit foundation, open-source community, *and* a tech company. We build the open-source Firefox web browser, Mozilla VPN, and products like Solo, an AI-powered website builder for micro-SMBs and solopreneurs. These products are used by hundreds of millions of individuals around the world. Mozilla's mission is to ensure the Internet is a global public resource, open and accessible to all. To fulfill this mission, we are constantly investing in the security of our products, the privacy of our users and in advancing the movement to build a healthier internet. This includes supporting research in areas like *competition* and the impact of *harmful social media recommendations* that have helped to inform policymakers around the world. Mozilla has *influenced* major companies to adopt better privacy practices and empowered people directly with *tools* to better understand and protect their data online. For Mozilla, individuals' security and privacy on the Internet are fundamental rights and must not be treated as optional.

With this goal, for the *past five years* Mozilla has been committed to advancing trustworthy AI. Mozilla recently published a paper, *Accelerating Progress Toward Trustworthy AI,* that outlines how Mozilla and our allies are advancing openness, competition, and accountability in AI. Mozilla is putting its resources behind these priorities as well: The Mozilla Foundation, which is the full owner of the Mozilla Corporation, has been dedicating 100 percent of its $30M a year budget to philanthropic activities, advocacy, and programmatic work on this topic. Mozilla is also investing another $30M in research and development on trustworthy AI, $35M in responsible tech startups—including startups with a focus on trustworthy AI—through *Mozilla Ventures,* and building the data infrastructure needed to create AI that works in multiple languages via *Common Voice.* We're seeking to help ensure that every person and every community can safely build, use, and assess AI.

The Imperative of Comprehensive Privacy Legislation

At Mozilla, we believe that comprehensive privacy legislation is foundational to any sound AI framework. Without such legislation, we risk a "race to the bottom" where companies compete by exploiting personal data rather than safeguarding it. Maintaining U.S. leadership in AI requires America to lead on privacy and user rights.

Privacy is a critical component of AI policy, not just because AI has the potential to accelerate privacy related harms, but because at its heart, AI is made possible by the utilization of tremendous amounts of data. How that data is collected today by AI companies varies, but there is little question that AI, especially generative AI, has created a dynamic that pushes companies to collect as much data as possible, creating a race to accumulate vast swaths of data.

In this context, any additional data a company can collect, including proprietary and personal data, could become a key competitive advantage as companies try to create "data moats," to ward off would-be competitors. This means that without regulation, business incentives will drive companies to collect more and more data however they can. For example, big tech companies could collect even more user data to train AI models, while data brokers would be incentivized to scoop up additional data to sell to third parties with AI ambitions, as the value of data increases.

AI systems thrive on data, and the drive to develop advanced AI models has intensified the demand for vast amounts of personal information. This data collection, often done without adequate consent or deceptive choices, poses significant risks to individual privacy and security.

By championing policies that promote innovation, create clear rules of the road for companies, and protect fundamental user rights, we can create both a competitive and level playing field for the American AI industry and prepare domestic champions for global leadership. At the core of these policies should be data minimization.

Data Minimization: A Cornerstone of Privacy and AI Policy

Data minimization is a crucial principle that ensures only the necessary data is collected and used for specific purposes—minimizing risk for business and enhancing consumer trust. This approach reduces the risk of privacy breaches, limits the potential misuse of personal information, and mitigates the burden of consumers having to defend their own privacy. In the context of AI, data minimization can be achieved through several strategies including:

1. *Informed Consent:* Individuals must be meaningfully informed about how their data will be used and be asked explicit consent when their personal data is used to train AI models. This transparency builds trust and empowers users to make informed decisions about their personal information while providing clarity to businesses. Mozilla has *campaigned* on behalf of consumers to push the industry to do better when it comes to transparency.
2. *Privacy by Design:* Integrating privacy considerations into the design and development of AI systems ensures that privacy is not an afterthought but a fundamental component. This holistic approach of privacy by design—encompassing the entire AI lifecycle, from data collection to deployment—is a core element of Mozilla's recent "Privacy for All" *campaign.*

Investment in Privacy-Enhancing Technologies

While legislation is essential, technical advances must work hand-in-hand with them to create a more safe and private future. The ecosystem needs significant investment in privacy-enhancing technologies (PETs) to develop AI systems that respect and protect individual privacy. PETs enable innovative solutions that reduce risk in the AI lifecycle while ensuring privacy is maintained without stifling technological progress. For example, PETs can enable training and processing on-device or

obfuscate machine learning outputs via differential privacy to mitigate the risks of re-identification.

At Mozilla, we are committed to advancing privacy-preserving approaches in both the browser and for AI in general. We are focused on developing tools that prioritize user privacy by running on user devices (via projects such as *Llamafile*) and by developing technologies such as *Interoperable Private Attribution* (IPA) that minimize the need for data collection via browsers by leveraging multi-party computation. *Local or on-device processing* enables AI models to run on local devices rather than centralized cloud servers, significantly reducing the amount of data transmitted and stored by service providers. Mozilla's AI-enabled *translation feature* in Firefox, for example, performs translations locally using machine learning—ensuring that user data (such as page URLs and content) is not sent to either Mozilla or third-party servers who can then use data collected for their own purposes.

The Role of Openness in Privacy-Preserving AI

Openness is an essential ingredient for improving verifiable and meaningful privacy in AI technologies. While there are different degrees in the spectrum of openness, making AI components and systems more openly available to the wider community, improves transparency. Transparency, in turn, enables scrutiny—without which we have little ability to govern and hold the current large models to any privacy standards we might expect of other online businesses.

Without knowing what data is being collected and how it is being leveraged by AI systems, we will have little ability to govern the technology effectively in the interests of consumers. Without incentives that encourage openness across the AI stack, a handful of dominant companies will win the race to the bottom, while citizens lose any effective means of control over their privacy.

Open approaches also play a vital role in promoting innovation, preventing the concentration of power in the hands of a few companies. They enable the economic benefit of AI to be more widely shared, amongst businesses of different sizes and capabilities—leading to increased investment and job creation. We also have clear *evidence* from open source development practices, that openness allows for diverse input and collaboration, fostering the development of privacy-preserving techniques that can benefit everyone rather than relying on security through obscurity.

Mozilla's commitment to openness is exemplified by our efforts to enable AI models to run on private devices with private data, via projects such as *Llamafile.* This reduces the need for data to be sent to centralized servers, mitigating privacy risks and promoting user control.

AI Can Amplify Privacy Violations

Online manipulation, targeted scams, and online surveillance are not new risks in our digital lives. Bad actors often seize on any opportunity they can, whether through spam e-mails or sophisticated deep fakes, to harm the average American. However, AI technologies can supercharge such harms by enabling personalization and scale with much lower barriers to access such capabilities than previously possible. AI technologies introduce unique privacy challenges that must be addressed proactively, where some of the most pressing concerns include:

- *Profiling and Manipulation:* AI can infer sensitive attributes about individuals, leading to potential privacy violations if used for targeted content or discrimination. This is especially true for advertising, a field where AI and machine learning have already been leveraged for years to predict the wants and desires of unsuspecting consumers. In addition, the growth of generative AI has led to advertisers creating highly customized campaigns, from text to images to videos, raising the likelihood of hyper-targeted manipulation at low costs.
- *Consent and Data Rights:* Using personal data to train AI models raises questions about consent, especially when individuals are unaware their data is being used for training. In the case of sensitive categories, such as kids or health data, existing protections need to be updated for newer use cases that AI enables. These updates can include stricter anonymization standards, inclusion of data inferred by AI systems (such as behavioral profiles and predictive analytics), and improved disclosure requirements for when such sensitive data is leveraged for training AI models.
- *Bias and Discrimination:* AI systems trained on biased data can perpetuate and amplify these biases, resulting in discriminatory outcomes. We've already seen prominent companies be taken to *court* for such practices by the U.S. government and AI will only create more avenues for such algorithmic discrimination.
- *Data Exploitation:* Generative AI systems trained on vast datasets may inadvertently reveal private information, posing risks to the privacy and security of

the average American or for businesses whose employees use such systems. For example—employees using a cloud-based generative AI platform to create meeting notes by feeding in potentially sensitive or confidential information could inadvertently lead to that platform leaking that data to other parties in the future, something we've already seen *occur* in the recent past.

- *Deepfakes and Identity Misuse:* AI-generated content can convincingly depict individuals doing things they never did, threatening privacy and reputation.

To mitigate these risks, we need comprehensive Federal privacy legislation, strong regulatory oversight, and continued investment in PETs. We must also ensure that AI systems are transparent and accountable, with mechanisms in place to address privacy violations and provide recourse for affected individuals, underpinned by disclosure.

Protecting Civil Liberties in the Age of AI

AI's potential to impact civil liberties cannot be understated. The same technologies that drive innovation can also be used to infringe upon fundamental rights and used by big tech companies to trample individuals' privacy. Therefore, it is imperative that AI development and deployment are guided by principles that protect civil liberties. This includes safeguarding freedom of expression, preventing unlawful surveillance, and ensuring that AI systems do not perpetuate discrimination or bias.

At Mozilla, we have long championed the protection of civil liberties. We believe that privacy is not just a feature but a fundamental right that must be upheld in all technological advancements. Our commitment to privacy preserving data practices and AI reflects our dedication to protecting users' civil liberties in the digital age.

The Path Forward

As we navigate the complexities of AI and privacy, it is crucial to strike a balance between innovation and protection. Regulation must be designed to address the root causes of AI-enabled societal harms without entrenching the position of a few dominant players. We should avoid restrictive licensing regimes that could stifle competition and innovation, particularly for small and medium-sized enterprises (SMEs) and open-source developers.

Instead, we need a regulatory framework that promotes responsible AI development and deployment, safeguards individual privacy, and fosters a diverse and competitive AI ecosystem. This includes urgently creating clear rules and enforcement mechanisms to stop bad actors from exploiting the innate privacy rights of Americans' online. America can continue to be a leader in AI by putting in place clear rules of the road on privacy and data protection that will help to spur beneficial competition and create a level playing field for players of all sizes instead of a race to the bottom. The improved consumer trust engendered by better privacy practices leads to increased brand loyalty, enhancing the competitive edge that American technology companies currently enjoy globally. Robust privacy practices also attract international partnerships and investments, positioning businesses to compete more effectively in the global marketplace—where privacy is increasingly a competitive differentiator.

Conclusion

In conclusion, protecting Americans' privacy in the age of AI is a critical challenge that requires comprehensive legislation, policies that support openness, investment in privacy-enhancing technologies, and a commitment to data minimization. At Mozilla, we are dedicated to advancing privacy-preserving AI and advocating for policies that promote innovation while safeguarding individual rights.

We urge Congress to pass binding Federal privacy legislation and enforce strong privacy regulations. By doing so, we can ensure that AI development proceeds in a manner that respects privacy, promotes trust, and benefits all Americans.

Thank you for the opportunity to testify today. I look forward to your questions and to working with you to protect Americans' privacy in the AI era.

The CHAIR. Thank you, Mr. Tiwari. I very much appreciate you being here.

And, Mr. Reed, thank you so much for being here. I am not trying to ask you a question in advance but I am pretty sure you have thousands of members of your organization, and I am pretty sure you have quite a few in the Pacific Northwest.

So thank you for being here.

STATEMENT OF MORGAN REED, PRESIDENT, ACT | THE APP ASSOCIATION

Mr. REED. We do, many in the great state of Washington.

Chair Cantwell, Ranking Member Cruz, and members of the Committee, my name is Morgan Reed, President of ACT | The App Association, a trade association representing small and medium sized app developers and connected device manufacturers.

Thank you for the opportunity to testify today on two significant and linked subjects, privacy and AI.

Let me say very clearly that the U.S. absolutely needs a Federal privacy law. For years we have supported the creation of a balanced, bipartisan framework that gives consumers certain protections and businesses clear rules of the road.

Instead, what we have now is a global array of mismatched and occasionally conflicting laws including here in the U.S. with either 19 or 20, depending on who you ask, state-level comprehensive privacy laws and more coming every year.

To prevent this morass of confusion and paperwork, preemption must also be strong and without vague exceptions and it must include small businesses so that customers can trust the data is being protected when they do business with a company of any size.

Unfortunately, the American Privacy Rights Act, or APRA, falls short of both of these objectives. Carving out small businesses from the definition of covered entities as APRA does is a nonstarter because it would deny us the benefits of the bill's preemption provisions.

Instead, small business would be required to comply separately with 19 state laws and, more importantly, the not yet passed laws in 31 states, exposing us to costly state-by-state compliance and unreasonably high litigation costs.

And it is not just small tech impacted by this. In today's economy everyone uses customers' data, even bricks and mortar. A local bike shop in Nevada likely has customers coming from Utah, Arizona, California, Colorado, and Idaho. An alert reminding these customers about a tire sale with free shipping or that it is time to get their bike in for a tune up requires at least a passing familiarity with each state's small business carve out.

In the ultimate irony, APRA may even incent small businesses to sell customers' data in order to gain the benefit of preemption. Congress must instead move forward with a framework that incorporates small businesses and creates a path to compliance for them.

And this acceptance of small businesses' role in the tech ecosystem becomes even more pronounced when we turn to AI. Mainstream media is all abuzz about big companies like Amazon, Microsoft, Google, and Apple moving into AI but the reality is small business has been the faster adopter.

More than 90 percent of my members use generative AI tools today with an average 80 percent increase in productivity and our members who develop those AI solutions are more nimble than larger rivals.

We are developing, deploying, and adapting AI tools in weeks rather than months. Their experiences should play a major role in informing policymakers on how any new laws should apply to AI's development and use.

Here are two examples of how our members are using AI in innovative ways. First up is our Iowa-based SwineTech. It is reshaping the management of hog farms.

Farmers use their product PigFlow—that is really the name—to manage the entire process of using sensors to track the health of a thousand piglets and then market analytics and public information to build AI-powered holistic solutions.

But, as Paul Simon said, "big and fat, a pig's supposed to look like that." For our member MetricMate in Atlanta the goal is the opposite. This Atlanta-based startup uses a combination of off-the-shelf and custom fitness trackers to help individuals and physical therapists to track and refine fitness goals.

AI helped MetricMate respond to the progress being made over time and instantaneously while their patented tap sensor gives the user the ability to track their workouts and seamlessly transmit data to the MetricMate app.

These examples show how AI is useful for innovative yet normal activities. So rather than limit AI as a whole, policymakers must target regulation to situations where a substantial risk of concrete harm exists.

The risk of AI use on a pig farm should not be treated the same as risks in sectors like health care or wellness, and yet both of them might be covered by future laws.

Finally, I want to stress the importance of standards to the future of AI. Standards are a valuable way for new innovators to make interoperable products that compete with the biggest market players.

As the Committee considers bills on the subject we need NIST to remain a supporter rather than an arbiter of voluntary industry-led standards. The committee should also be aware of the threat to small business through standard essential patent abuse.

With non-U.S.-based companies holding the crown for the most U.S. patents every year, Federal policy must combat abuse of patent licensing in standards by ensuring that licenses are available to any willing licensee including small businesses on fair, reasonable, and nondiscriminatory terms.

If we are not capable of doing that the next generation of AI standards will not be owned or run through U.S. companies but through those outside of the U.S. with different perspectives on human rights and our expectations.

So thank you for your time, and I look forward to answering your questions.

[The prepared statement of Mr. Reed follows:]

PREPARED STATEMENT OF MORGAN REED, PRESIDENT, ACT | THE APP ASSOCIATION

I. Introduction

Small app companies and connected device makers use, create, or adapt artificial intelligence (AI) tools every day. Their activities involve a variety of different kinds of AI, from machine learning and deep learning to generative AI tools such as foundation models (FMs), large, medium, and small language models (LMs), and image generators. In creating, tuning, and leveraging these tools, ACT | The App Associa-

tion's (the App Association's) members are keenly aware of the risks these tools may present, including how their processing activities meet customers', clients', and users' privacy and security expectations. In turn, innovators in the app economy must be able to rely on business partners, distributors, and online marketplaces that enable the best privacy and security protections.

AI refers not to a single program or use case, but to a broad category of general-purpose technologies that companies and consumers are applying to new challenges every day. Because of this, policymakers must narrowly target government intervention to situations where a substantial risk of concrete harm exists, tailored to the harms at issue. Just as Congress declined to create a specific Federal agency to regulate combustion engines in all their manifestations, it should also focus its AI efforts on how the technology is used and provide the flexibility to scale measures taken to address the risks presented by different scenarios. For example, the risks presented by AI used to improve the quality of pizza are fundamentally of a different nature than those presented by clinical decision support tools in healthcare. Consistent with our policy principles on AI (see Appendix),[1] Congress must first look to existing statutes, regulations, and best practices and understand how they apply to emerging technologies before leaping forward with legislation. We agree with several Federal agencies that recently affirmed that their jurisdictional boundaries do not end where the use of AI begins. There is no "AI shaped hole" in the Federal Trade Commission (FTC) Act; unfair or deceptive acts or practices taking place with the help of AI or regarding AI services are just as prohibited as their unassisted analogues. Overall, the risks AI poses are not fundamentally new and overbroad intervention to control the development of the technology is unlikely to produce the results policymakers seek.

The scope of this hearing is appropriate, as the development and use of AI adds to the urgency for Congress to legislate on privacy in particular, while some other areas are not as ripe for substantive intervention. Our testimony makes three overarching points:

1. *The United States needs a Federal privacy law.* On the one hand, the United States is several steps ahead of other countries in the development of AI sectors, in part because it has thus far declined to overregulate privacy. On the other hand, our innovation economy could fare even better on the global stage if Congress were to enact a strong, preemptive Federal privacy framework that bolsters trust in cutting-edge AI tools while curbing mismanagement of personal data.
2. *Small companies are the leading edge on AI.* Nimbler than their larger rivals, small businesses in the app economy have a comparative advantage in developing, deploying, and adapting AI tools for a variety of purposes. Their experience is a primary shaping force in the development of FM services and generative AI in all of its various forms and should play a major role in informing policymakers on how any new laws should apply to AI's development and use. They also benefit from a competitive landscape in markets for LM and FM services. They do not want policymakers to prematurely intervene on antitrust grounds, a development that could ironically stifle competition on the features small businesses care about most.
3. *Standards are going to play an important role in AI and other emerging technologies.* Small businesses leverage standards every day to compete with larger rivals and to interoperate with products and services that they can build on. The National Institute for Standards and Technology (NIST) plays an important role as a participant in voluntary, industry-led standards development efforts, as a clearinghouse of information on standards development, and as a coordinator of Federal government participation in industry-led processes. However, Congress must encourage NIST's leadership in preserving small businesses' access to standardized technologies by holding standard-essential patent (SEP) holders to their commitments to license SEPs to any willing licensee on fair, reasonable, and non-discriminatory (FRAND) terms.

II. A Federal Privacy Framework

The proliferation of AI tools across industries and around the world is one of the most important reasons for Congress to establish a single, preemptive Federal privacy framework. While a restrained approach to governance should guide Congress' thinking on AI as a group of technologies, Congress has a more developed understanding of the privacy questions at issue with their adoption. With 19 state-level

[1] ACT | THE APP ASSOCIATION, POLICY RECOMMENDATIONS FOR AI, available at *https://actonline.org/wp-content/uploads/Policy-Recommendations-for-AI.pdf.*

comprehensive privacy frameworks in place, Europe's General Data Protection Regulation (GDPR), and a host of other regulatory regimes in various stages of consideration and implementation, privacy is a good fit for congressional action.

The privacy risks AI poses are outgrowths of existing privacy issues. Privacy is concerned first and foremost with the universe of purportedly *authorized* collection, processing, and transfer activities an entity may pursue. The impracticability of a single consumer understanding and authorizing all the foreseeable uses of data across all of the services they access—coupled with the elusiveness of defining privacy harms—have long presented formidable challenges for policymakers approaching the privacy problem. With AI, these same challenges emerge, but on a larger scale and with greater intensity on the foreseeability factor. For small businesses, the twin imperatives to provide regulatory clarity and to avoid taking away the tools they use now are heightened. With these considerations in mind, it may help to describe small businesses' priorities for federal privacy legislation, with a special focus on AI and with the American Privacy Rights Act (APRA) as a reference.

Data minimization. AI is often useful precisely because it surfaces insights or ideas that people are unable or less inclined to find on their own. Therefore, the purpose the data serves, for both the entity processing it and the individual to which it pertains, often evolves after its initial collection. For small businesses, a data minimization provision that imposes a blanket ban on processing of personal data, except in specifically enumerated circumstances, is likely to cause problems. Both GDPR and APRA impose such a ban on processing, unless specific lawful bases exist. GDPR's formulation is more permissive, as it allows processing that is "necessary for the purpose of the legitimate interests pursued by the controller or by a third party" and where the "data subject has given consent to the processing" for "specific purposes."[2] In general, data minimization provisions should take the opposite approach, avoiding a blanket ban on all processing while describing prohibited processing activities that are likely to cause net concrete harm. Those concrete harms are not necessarily limited to financial or physical harms; then-Acting Chair of the FTC Maureen Ohlhausen's useful 2017 taxonomy of recognized harms outside those categories, including reputational injury and unwarranted intrusion, is still applicable.[3] Consistent with these concepts, if Congress proceeds with proscriptions on processing activities, we recommend the use of relevant context and consumers' reasonable expectations as twin touchstones. The extent to which processing of personal data respects the reasonable expectations of consumers given the context in which data processing takes place is often the best predictor of possible risk of privacy harms occurring.

Explicit small business treatment. In legislatures across the country, proponents of privacy measures have indicated a desire to ensure small businesses are able to comply with and are not unduly burdened by any applicable requirements. However, we believe that APRA's specific method of achieving that goal—carving out small businesses from the definition of "covered entity"—could potentially deny them the benefits of preemption and inadvertently expose them to costly state-by-state compliance and unreasonably high litigation risks from differing liability regimes.

By excluding small businesses from the definition of covered entity, APRA would create uncertainties as to whether small businesses would be covered by the bill's preemption provision—or if, instead, they would remain regulated by existing and future state privacy laws. If small businesses are not covered entities under APRA's preemption provision, which preempts state laws "covered by" the Federal law, they may have to contend with a burdensome patchwork of state privacy laws while their larger counterparts enjoy a single privacy standard. If the Committee is worried about further entrenching larger companies with big compliance budgets while disadvantaging smaller companies, we believe a pure carveout would have exactly this effect.

As we have previously indicated in testimony, App Association members are not asking to be carved out of Federal data privacy legislation.[4] Instead, requirements

---

[2] Gen. Data Protection Reg., Art. 6, available at *https://gdpr-info.eu/art-6-gdpr/*.

[3] Hon. Maureen K. Ohlhausen, Acting Chair, Fed. Trade Comm., "Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases," speech before the Fed. Comm'cns Bar Assoc. (Sept. 19, 2017), available at *https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.*

[4] "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security," hearing before the House Committee on Energy and Commerce, Subcommittee on Consumer Protection and Commerce, (117th Cong., 2d Sess.), statement of Graham Dufault, senior dir. for public policy, ACT | The App Association, available at *https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-DufaultG-20220614.pdf* ("The safe harbor would ensure that App Association members are rightfully viewed as—and held accountable for—complying with a Federal framework. . .").

should be scalable depending on the size, nature, and complexity of an enterprise's processing activities, and small businesses should have access to compliance programs that provide a presumption of compliance with the law. We note that some of the world's largest companies have had to make prodigious compliance investments to meet GDPR requirements that are simply beyond the reach of App Association members. For example, Google's chief privacy officer testified before this Committee in 2018 that the company had to invest "hundreds of years of human time" to come into compliance with the framework.[5] Offering small businesses a path to compliance is essential to ensuring the law holds them accountable, but that they have some protection from nuisance lawsuits and are afforded reasonable opportunities to rectify compliance issues in good faith. A compliance program would ensure that App Association members are rightfully viewed as—and held accountable for—complying with a Federal framework, while alleviating excessive liability concerns and other burdens.

Preemption. Preemption must be strong and without vague exceptions. The great economic benefit of the Internet is that it has allowed small businesses to reach customers in all 50 states. Small businesses do not, however, have the time or capacity to conduct constant legal analyses to determine whether relevant state law or Federal law applies to their activities with each new scenario presented. Therefore, a preemption provision should expressly preempt state laws "related to" the Federal law and should not have exceptions that call into question Congress' intent with respect to preemption.

Private right of action (PRA). A Federal privacy framework must avoid inadvertently creating new sue-and-settle business models and inviting other abusive tactics based on claims with no merit. We acknowledge that the difficulty in bringing suit under current law lies in defining the harm that accrues to the aggrieved consumer. But, even under a new Federal regime, in the majority of cases, enforcement agencies are equipped to obtain redress to the extent it Is warranted. Therefore, we do not believe a PRA is a necessary element of a comprehensive Federal privacy framework. However, if a bipartisan Federal privacy bill includes a PRA, several safeguards are necessary: remedies must not include statutory per-person, per-violation monetary damages; any violation of the law should not constitute an injury-in-fact; businesses must be allowed an opportunity to cure the alleged problem before a suit is allowed to proceed; there must be penalties for baseless claims; and Congress should require notice to Federal or state enforcement agencies, empowering them to veto baseless claims.

III. How Small App Companies and Connected Device Makers Use, Develop, and Adapt AI Tools

The reality of AI use in everyday marketplaces is both less shocking and more interesting than headlines and handwringers suggest. For example, focusing on the most egregious instances of facial recognition misuse by law enforcement agencies would provide an inadequate basis for understanding how AI works in the vast majority of commercial cases and the risks it truly presents. An overview of how App Association members use AI in diverse ways may provide a more helpful and representative sample of how AI benefits people and the kinds of risks at issue. For a lengthier report on our member companies' perspectives on and uses of AI, our white paper, *Small Businesses and Entrepreneurs: An Indispensable Force in the AI App Economy,* describes further examples from members in the United States and overseas.[6]

In a recent App Association member survey, 75 percent reported using generative AI.[7] The figure for all kinds of AI is likely close to 100 percent, and since that survey was conducted late last year, the number using generative AI has likely increased. Many App Association members are also on the developer side of AI tools, and some even make the connective tissue for developers to customize LM resources for specific purposes. Among a range of enterprises, another survey recently revealed that among those that deploy large LMs, only 3 percent use just one, while

---

[5] Ashley Rodriguez, "Google says it spent "hundreds of years of human time" complying with Europe's privacy rules," QUARTZ (Sept. 26, 2018), available at *https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr#:~:text=Google's%20chief%20privacy%20officer%2C%20Keith,company%20into%20compliance%20with%20GDPR.*

[6] ACT | THE APP ASSOCIATION, SMALL BUSINESSES AND ENTREPRENEURS: AN INDISPENSABLE FORCE IN THE APP ECONOMY (Fall 2023), available at *https://actonline.org/wp-content/uploads/small-businesses-and-entrepreneurs-an-indispensable-force-in-the-ai-app-economy.pdf.*

[7] Priya Nair, "Survey Says: AI and IP are Essential to Innovation," ACT | The App Association Blog (Feb. 27, 2024), available at *https://actonline.org/2024/02/27/survey-says-ai-and-ip-are-essential-to-innovation/.*

83 percent use three or more.[8] Summarizing the reason for this variety, one of the respondents said, "[f]or about 50 percent of use cases, we use OpenAI, for 30 percent—40 percent of use cases, we use our internal fine-tuned and pre-trained LLMs based on open-source LLMs like Llama 2 or Mistral, and for others we use Anthropic or Cohere."[9] Looking at the broader marketplace, the internal fine-tuned segment is especially common and an area where App Association members play a significant role, as they and their clients use AI to help them be more efficient at what they do not necessarily do that well so that they can focus on what they *do best.* As generative AI's lifecycle transitions from hype to rubber meeting road, these smaller models are emerging as the more realistic immediate use case for enterprises around the world.[10] For their part, small businesses say they are motivated to adopt AI tools primarily for cost savings and due to competitive pressure, and the most common uses by small businesses for AI tools are financial management, e-mail marketing automation, and to enhance cybersecurity capabilities.[11]

Decision support: healthcare. One of our member companies recently built a simple, AI-driven tool that both expands options for small healthcare practices and helps invigorate competition in a key market for practice management systems (PMS). These systems help healthcare practices manage their patient intake processes and are especially important for scheduling and managing contact and communications with patients. It can be especially difficult for small practices to find the right PMS that fits their specialty or patient population. Our member built the tool to rapidly scan and analyze broader range of PMS options on the market and rank them in terms of which would be the best fit for the client practice. It is an excellent example of AI made by small businesses for small businesses, helping solve a targeted problem and providing a custom solution in a manner that improves efficiency.

Caregivers have used clinical decision support (CDS) tools to help accurately diagnose conditions and build treatment plans that best fit their patients. App Association member Rimidi provides a remote physiologic monitoring and clinical decision support platform for patients and their providers to manage a variety of chronic conditions.[12] Rimidi helps ensure that providers can intervene when necessary when a patient's diabetes is at risk of reaching uncontrolled levels and helps chart a management plan that fits unique patients and their symptoms.

Generative AI. Real-world LM deployment is typically not a case of workers punching a prompt into ChatGPT and copying and pasting the results. For example, App Association members adapt LMs to draft marketing materials and write code. They start with either licensed or open-source models and fine tune them to produce results that better fit the results they want. Fine-tuning can also help an organization ensure a LM's outputs hew more closely to ethical and legal requirements, reducing the editing and review burden on the people in the loop.

In another example, App Association member Rotational Labs creates custom plug-ins for their clients to maximize their use of available LMs. They also help create "domain-specific" LMs using open-source models, allowing their clients to create their own models with their own data, either on a provided cloud infrastructure or the client's existing service. For one client, Rotational built a custom domain-specific model that successfully reduced manual review of tens of thousands of news articles by 90 percent.[13]

Decision support: financial services. Common in industries from fast food to healthcare, AI decision support tools have reached virtually every part of the economy. App Association members are redefining productivity by building and servicing decision support options driven by AI. For example, Florida (and Washington)-based Devscale built Clockwork.ai, a data visualization and decision support platform for financial professionals.[14] The tool integrates with commonly used bookkeeping software to provide projections and "crunch numbers" while their clients can focus on relationships and expanding their business. Clockwork is, in turn, able to save its clients over 10 hours per month and help them grow their enterprises by 50 per-

---

[8] CBCINSIGHTS, STATUS: OPEN RELATIONSHIP, available at *https://tinyurl.com/58y7bezu.*

[9] *Id.*

[10] Tom Dotan and Deepa Seetharaman, "For AI Giants, Smaller Is Sometimes Better," THE WALL STREET J. (JUL. 6, 2024), available at *https://www.wsj.com/tech/ai/for-ai-giants-smaller-is-sometimes-better-ef07eb98.*

[11] SBE COUNCIL, SMALL BUS. AI ADOPTION SURVEY, (Oct. 2023), available at *https://sbecouncil.org/wp-content/uploads/2023/10/SBE-Small-Business-AI-Survey-Oct-2023-FINAL.pdf.*

[12] RIMIDI, available at *https://rimidi.com.*

[13] ROTATIONAL LABS, CASE STUDY: BLUEVOYANT, available at *https://rotational.io/case-studies/blue-voyant/.*

[14] DEVSCALE, CASE STUDY, CLOCKWORK, available at *https://devscale.com/casestudy/clockwork/.*

cent.[15] This is an example of a deployment that does not draw on large LMs or FMs, but still uses machine learning to generate recommendations for users.

Decision support: pizza quality. Other kinds of decision support tools have been around for longer and are developed in-house. Domino's Pizza began training their DOM Pizza Checker in 2019, inviting customers to take pictures of their pizza in exchange for redeemable points.[16] Domino's trained DOM with 5,000 images of pizza on an NVIDIA DGX platform and deployed it in 2021. The system captured pizzas as they left the oven, assessing each for pizza type, correct toppings, topping distribution, and aesthetic appeal. The system can flag a finished pizza that is likely to generate a consumer complaint, enabling store management to quickly identify and address quality issues as they arise. Domino's says the quality of their pizza has improved 14 to 15 percent in the stores that have deployed DOM.

Decision support: smart agriculture. App Association members are also modernizing agriculture with software, smart devices, and AI. For example, Honolulu-based Smart Yields connects farmers and agricultural researchers to increase crop yield, revenue, and productivity. In a case study conducted with the Kohala Institute, Smart Yields embedded their sensors into the water system and soil around different crop fields, allowing for maximized water usage, better understanding of erosion and soil management, and an overall reduction in agricultural waste. Their use of retrofitted monitoring collars on local pig populations and a related algorithm that helps to monitor and predict herd movements has allowed farmers in the area to better protect their crop, especially macadamia nuts, while still preserving the land and safety of these native animals critical to the overall health of the local ecosystem. Smart Yields is helping Hawaii meet their commitment to doubling food production by 2030 and other communities achieve similar goals around the world.

Competition in the markets for LM and FM services. Taking stock of how small businesses use AI in practice, they tend to select the options that fit their specific purposes. As a result, they often rely on a combination of services and customizations of the raw models. Conceptions of the marketplace as dominated by a handful of firms behaving anticompetitively do not comport with their reality. While some commenters have cast the burgeoning market for LM services as locked in by large companies, the truth is that the future of the market for LM services is far from clear. Moreover, the market for AI services generally is robust, with plenty of competitors entering and competing successfully in the market.[17] These commenters' premises suggest Congress and other officials should do something to discourage or stop the participation of companies over a certain size in these markets. But small businesses stand to lose the most should artificial barriers to entry, such as imposing a licensing regime for FMs, be created in such policies. Small businesses also likely derive the most benefit from the creation of vertically integrated distribution and service offerings these companies are best positioned to provide. Ex ante regulations or enforcement actions designed to require strict interoperability or open access to LM services could also serve to eliminate the aspects of these services on which LM and cloud providers currently compete vigorously for App Association members' business, including privacy and security.[18]

Small businesses in the app economy are skeptical of government discouraging the investment of billions of dollars to create the infrastructure on which they plan to build their problem-solving innovations. Seemingly laying the groundwork for premature enforcement activity, the FTC's 6b study on generative AI markets[19] is concerning evidence of an intent to interfere with or control the extent to which small businesses are able to do business with their largest partners and clients. Small companies have invested and will continue to invest in creating LMs, but limiting the size of the companies with which they can transact for services that require significant investment is not fair to the small businesses that need those offerings to be robust. Similarly, small businesses do not want policymakers to forbid

---

[15] CLOCKWORK, available at *https://www.clockwork.ai/*.

[16] Heili Palo, "The Secret Surveillance Sauce to Domino's Pizza's Success," Assignment: Competing with Data, DIGITAL INNOVATION AND TRANSFORMATION, HARVARD BUS. SCHOOL (Mar. 28, 2022), available at *https://d3.harvard.edu/platform-digit/submission/the-secret-surveillance-sauce-to-dominos-success/*.

[17] See Kendrick Kai, "AI50," FORBES (Apr. 11, 2024), available at *https://www.forbes.com/lists/ai50/*.

[18] *See* Kedhar Sankararaman, "Unlocking the Future: How Smart Investments and Sensible Governance Can Propel the LLM Industry Forward," ACT | THE APP ASSOCIATION BLOG (Jun. 24, 2024), available at *https://actonline.org/2024/06/24/unlocking-the-future-how-smart-investments-and-sensible-governance-can-propel-the-llm-industry-forward/*.

[19] Fed. Trade Comm'n, press release, "FTC Launches Inquiry into Generative AI Investments and Partnerships," (Jan. 25, 2024), available at *https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships.*

them from partnering with their most lucrative clients and partners that happen to have the most powerful distribution channels. Thus, the government should not prevent or discourage larger companies with existing physical assets or know-how from moving vertically into FM and LM services.

Consider a parallel example. As the latest model cars take on more autonomous features, the industry is undergoing major shifts. New entrants are taking advantage of these disruptions to make credible inroads, while incumbent auto manufacturers are poised to leverage their existing vertical supply chains and manufacturing bases to make autonomous cars. Imagine if policymakers decided incumbent auto manufacturers should either be barred from making autonomous vehicles or regulated differently from market entrants just because they already have a vertically integrated advantage and compete successfully in the market for non-autonomous cars. Such a decision would deprive consumers of options from some of the strongest competitors and artificially box out years of experience in areas like safety.

Similarly, companies like Amazon, Microsoft, and Google have a sprawling network of existing assets in upstream industries such as cloud computing, which already serve as part of the vertical stack for LLMs and FMs. Just like building a car requires auto manufacturing capacity and a supply chain, LMs and FMs require significant computing power, and this is one of the main inputs for LM and FM services. In turn, cloud services are the main providers of this capacity. So, government intervention to prevent cloud companies from providing cloud capacity for their own FM efforts—or even to prevent them from providing compute capacity to other FM or LM projects—just because they are large incumbents in cloud computing appears to defeat the purpose of antitrust law.

IV. Standards are Critical for AI Technology Development

As technical standards are integrated into AI products and as AI standards form, a fair and balanced standards ecosystem will drive U.S. AI-based invention in critical sectors, including green technology and precision agriculture. We appreciate Congress' focus on this issue, as several members of this Committee have introduced measures aimed at enhancing American leadership in supporting the development and adoption of critical and emerging technology (CET) standards, which are—and will be—an important support of transformational AI-driven technologies around the world. Voluntary, open, private sector-led standards development has been a decisively winning approach for American technology interests. Any legislation to support this ecosystem must balance the interests of advancing American leadership with maintaining the openness of standards development organizations and the primacy of private sector leadership.

Among the measures introduced, we support the bipartisan *Promoting United States Leadership in Standards Act* (S. 3849), led by Senators Mark Warner and Marsha Blackburn.[20] We believe this legislation can better position standards development organizations and standards participants for success. A strong, yet nimble, approach to technical standards development is a foundational imperative for the App Association's members as they create tomorrow's innovations. Nurturing open and global participation in standardization activities, especially when hosted in the United States, can address shared technical challenges while advancing American technology leadership. If the Committee considers this legislation, we would like the authors to consider removing "prestandardization" and "standards coordination" from the activities supported by the funds that would be allocated for the grant program. NIST already undertakes these activities, as do private sector-led standards development organizations (SDOs). Thus, although NIST should have more resources, funds set aside for hosting meetings in the United States should not also be set aside for activities NIST is already undertaking.

With respect to the array of additional proposals and oversight issues affecting NIST and its role in standards development, we offer a couple of guiding principles:

NIST should remain a supporter, rather than arbiter, of international standards development. Any legislation must avoid unintentionally recasting NIST's longstanding role in standards development. Legislation should not task NIST with evaluating the merit of standards developed by SDOs or auditors checking on testing, evaluation, verification, or validation.

---

[20] Promoting U.S. Leadership in Standards Act (S. 3849, 118th Cong.), available at *https://www.congress.gov/bill/118th-congress/senate-bill/3849?q=%7B%22search%22%3A%22s+3849%22%7D&s=1&r=1.*

International collaboration. Legislation should avoid creating an appearance of convening a "voting bloc" that could cause the creation of competing blocs and lead to global fragmentation of standards development.

Standard-essential patent abuse. While the United States is the world leader in technology innovation, China is expanding its attacks, including through anti-competitive standard-essential patent (SEP) licensing abuses, which undermine the functioning of the open standards system. Originating in the telecommunications sector but now seen across key U.S. economic verticals, SEP abuse continues to be enabled by a lack of support and enforcement on the U.S. government's part, which in turn continues to prompt bad faith SEP licensor practices. In one common example of SEP abuse, certain SEP licensors have been known to commit to making SEP licenses available to any licensee on FRAND terms and then breaking those commitments by systematically seeking injunctions against willing and reasonable licensees. In another example, certain SEP licensors refuse to license their SEPs to innovators at the most appropriate point in a supply chain, instead only making their licenses available to downstream manufacturers, unilaterally deciding for entire value chains where licenses can and cannot be taken. Conduct like this demonstrably increases costs for consumers, wastes vast amounts of capital on litigation instead of innovation, and pulls the rug out from under small businesses that rely on being able to take a license in order to interoperate with CET standards.

Federal policy must combat this abuse by holding bad actor SEP licensors to their commitments to license to any willing licensee—including small businesses—on FRAND terms. NIST was previously a signatory on a Federal policy statement on SEP licensing that, unfortunately, mischaracterized Federal law as allowing SEP injunctions against willing licensees. Having withdrawn the statement, the Biden Administration has not issued a new one, but we believe the Executive Branch should adopt a new policy that accurately describes the interplay of standards, patent licensing, and competition laws, and provide certainty and clarity to the ecosystem that:

- *The FRAND Commitment Means All Can License.* A holder of a FRAND-committed SEP must license that SEP to all companies, organizations, and individuals who use or wish to use the standard on FRAND terms.
- *Prohibitive Orders on FRAND-Committed SEPs Should Only Be Allowed in Rare Circumstances.* Prohibitive orders (federal district court injunctions and U.S. International Trade Commission exclusion orders) should not be sought by SEP holders or allowed for FRAND-committed SEPs except in rare circumstances where monetary remedies are not available.
- *FRAND Royalties.* A reasonable rate for a valid, infringed, and enforceable FRAND-committed SEP should be based on the value of the actual patented invention itself, which is separate from purported value due to its inclusion in the standard, hypothetical uses downstream from the smallest saleable patent practicing unit, or other factors unrelated to invention's value.
- *FRAND-committed SEPs Should Respect Patent Territoriality.* Patents are creatures of domestic law, and national courts should respect the jurisdiction of foreign patent laws to avoid overreach with respect to SEP remedies. Absent agreement by both parties, no court should impose global licensing terms on pain of a national injunction.
- *The FRAND Commitment Prohibits Harmful Tying Practices.* While some licensees may wish to get broader licenses, a SEP holder that has made a FRAND commitment cannot require licensees to take or grant licenses to other patents not essential to the standard, invalid, unenforceable, and/or not infringed.
- *The FRAND Commitment Follows the Transfer of a SEP.* As many jurisdictions have recognized, if a FRAND-committed SEP is transferred, the FRAND commitments follow the SEP in that and all subsequent transfers.

To advance the Congress' laudable goals of solidifying American leadership and elevating small businesses' freedom to innovate, strong enforcement against well-demonstrated SEP abuses is necessary. As foreign courts diverge on whether and to what extent to respect U.S. domestic law as it applies to SEP remedies, the Federal government cannot afford to relinquish its long-standing leadership position on SEP issues. Our own national interests would be best served by taking a strong stand against SEP abuse, particularly around CET standards, and we believe the Administration's National Standards Strategy for Critical and Emerging Technologies (NSSCET) implementation offers prime opportunities to establish this leadership.

V. Conclusion

Small businesses are leading the way in defining AI's beneficial uses and developing ways of managing and avoiding the risks presented. With their comparative advantage in speed and agility, the experiences and perspectives of small app companies and connected device makers provide a realistic picture of how AI is used in everyday commerce. We deeply appreciate that this Committee considers these perspectives as part of its inquiry into the risks and benefits of AI and how Federal privacy law may affect them. We look forward to working with the Committee to ensure that small businesses can continue to innovate on a strong foundation of privacy protection, standards access and development, and a free market with ample opportunities.

APPENDIX A

Majority Members

Maria Cantwell, Washington (Chair)

Headquartered in Seattle and founded in 2008, Digital World Biology creates digital educational tools to help students learn modern biology. Their app, Molecule World, is an easy-to-use visualization of 3D molecular structures ready for classroom use upon download. They also have a variety of textbook-like materials that help students learn quickly with visual aids and assist teachers with keeping students engaged with hands-on activities throughout the chapters.

Amy Klobuchar, Minnesota

Located in the Twin Cities and founded in 2013, Vēmos is a platform solution for bars, restaurants, and other venues as a one-stop-shop for the digital tools needed to manage and grow their businesses. Operating with only nine full-time employees, Vēmos found a way to harness and present a venue's data in a humanized way, which helps venues understand who their customers are and how to market to them effectively.

Brian Schatz, Hawaii

Founded in 2015 and headquartered in Honolulu, Smart Yields is an intelligent agriculture software that connects farmers and agricultural researchers to actionable real-time data, allowing them to increase crop yield, revenue, and productivity. With fewer than 10 employees, Smart Yields is committed to helping Hawaii meet its commitment to doubling food production by 2030 and other communities achieve similar goals around the world.

Ed Markey, Massachusetts

Established at the Massachusetts Institute of Technology (MIT) in 2011, Podimetrics is a medical technology services company that develops hardware-enabled, thermal-imaging solutions to predict and prevent diabetic foot ulcers. The Podimetrics SmartMat™ monitors the temperature of diabetes patients' feet to identify temperature asymmetries that signal the development of a foot ulcer. Coupled with a monitoring service, the Podimetrics Remote Temperature Monitoring System™ uses the wireless SmartMat™ to notify patients and clinicians of temperature asymmetry and inflammation, the first signs of foot ulcers, preventing amputations and other health complications.

Gary Peters, Michigan

With their U.S. operations based near Lansing, Michigan, Payeye has developed a unique eye-based payment method that combines hundreds of biometric data points within the iris and face to verify a customer's identity. They also offer express e-payments for e-commerce via QR codes and have developed a specific marketing and sales ecosystem centered around their technology.

Tammy Baldwin, Wisconsin

Based in Onalaska, Sergeant Laboratories is a software company that builds advanced IT security and regulatory compliance products for businesses. Their flagship product, AristotleInsight, measures and quantifies risk management data and provides detailed reports to compliance and security professionals to make informed decisions and stay a step ahead of cybercriminals.

Tammy Duckworth, Illinois

Aggieland Software is an IT consulting and custom software development company located in Springfield. The team at Aggieland Software helps their clients

achieve sustainable growth and efficiency through services involving blockchain, artificial intelligence, and software development.

Jon Tester, Montana

Headquartered in Bozeman, Guidefitter is an online and mobile platform that connects people with guides, nature experts, and sportspersons for safe and guided natural expeditions and sports, including hunting, fishing, hiking, and camping. The platform also allows the experts to promote their business or experience and facilitates payment for merchandise as well as the guided tour or event.

Kyrsten Sinema, Arizona

Founded in 2019, LiteraSeed is a digital health startup creating a visual way for patients to share their symptoms with their doctors. The product, called a "visual symptom report," focuses on helping patients whose first language is not English and those with lower literacy levels to communicate with their doctors and better understand their medical records.

Jacky Rosen, Nevada

Pigeonly is an online and mobile platform that connects inmates with their loved ones. Their services provide a central place to send letters, pictures, cards, and more. Through the platform, families can also call their inmate at a lower cost and stay in touch throughout their incarceration. The company's mission is to improve communication and community for those incarcerated and to encourage families to stay in touch with their inmates by simplifying and streamlining the process.

Ben Ray Luján, New Mexico

Snowball is an all-in-one fundraising platform that connects users with more than 15,000 nonprofits nationwide. The app has two parts. The first is for donors, giving them information about the nonprofits in Snowball's network, donation opportunities, and notice of emergency relief needs. It also provides a secure place to track donations and save credit card information. The second, for nonprofits, helps to keep track of donors, grow their donor base, and communicate fundraising opportunities.

John Hickenlooper, Colorado

Founded in 2007, Alchemy Security is a boutique cybersecurity firm based in the Central Rockies of Colorado. They serve as the cybersecurity expert for their clients, helping them make informed business decisions on how and where to invest valuable resources to minimize information security risks. Through a combination of risk analysis, security information and event management (SIEM), and other market-available technologies, Alchemy Security tailors their solutions to address the unique needs of their customers, regardless of industry or sector.

Raphael Warnock, Georgia

Based in Atlanta, Georgia, Rimidi creates mobile apps and software focused on supporting clinicians in the development of remote patient monitoring and chronic care management programs. Their clinical decision support tools, which work directly within existing electronic health records (EHR), combine patient-generated health data with clinical data allowing providers to make better-informed treatment and management decisions while also improving patient-engagement throughout care.

Peter Welch, Vermont

Aprexis Health Solutions is a cloud-based software that helps patients with personalized services for Medication Therapy Management and includes more than 1,000 participating pharmacies and more than one million patients. Founded in 2009, Aprexis works with health plans, pharmacy networks, corporate employers, and providers to deliver improved, patient-centric health outcomes.

Minority Members

Ted Cruz, Texas (Ranking Member)

Founded in 2018 by a trained speech pathologist, For All Abilities uses data to help employers amplify their employees' strengths while supporting their weaknesses through ADA/Disability 101 training and support throughout Equal Employment Opportunity Commission violation audits. Their main mission is to increase inclusion and equity for people with disabilities and help employers embrace the different abilities of employees.

John Thune, South Dakota

Infotech Solutions, LLC, is a concierge IT service helping businesses with everything from implementing a new software system or network to maintenance, general

IT issues, security, and more. The company also offers an app across platforms that helps their clients troubleshoot IT issues and connect with their IT service team remotely.

Roger Wicker, Mississippi

Alpha Victoria Studios, founded in 2016, is based in Gulfport and boasts a team of three creative engineers. This IT contracting business provides their clients with web and mobile software development, digital marketing, and search engine optimization services.

Deb Fischer, Nebraska

LyncStream, founded in 2012 in western Omaha, helps businesses of every size and industry use technology to grow and automate their business. They provide a litany of services, including database technology, web and mobile software development, and product management throughout the software lifecycle.

Jerry Moran, Kansas

Founded in 2014, Foster Care Technologies is an evidence-based support tool that helps inform placement decisions in foster care. Through their work with the University of Kansas School of Social Welfare, it was determined their product leads to better long-term placement outcomes for children in foster care, as well as reduced costs for agencies working on placement.

Dan Sullivan, Alaska

StepAway is a mobile application to help those with addiction manage their day-to-day and make better decisions about their daily habits to help prevent relapses. The app is primarily centered around those who are unable to seek addiction treatment services but are looking to make a change in their drinking habits. The app helps track daily progress while also giving users insight into their triggers and provides valuable information on how to make different and better decisions related to their alcohol use in a safe and private space.

Marsha Blackburn, Tennessee

Based in Nashville, Acklen Avenue provides clients with fully formed and outsourced software development teams. Founded in 2011, their services are tailored to each client's projects and staffing needs, making development a quick and efficient process whether the client is looking to develop a new aspect of an existing project launch or update.

Todd Young, Indiana

Located in Fishers, Arborgold is a software company helping landscaping businesses become more efficient and profitable since 1994. Their software encompasses job scheduling, resource management, profit margin estimations, and a series of mobile apps for employees to seek help regarding estimates, work orders, and other essential information.

Ted Budd, North Carolina

Founded in 1994 and headquartered in Chapel Hill with 26 employees,/n Software provides clients with the tools they need to build internet-enabled web and desktop applications. Software developers at most Fortune 500 companies use their flagship product, IPWorks, to build their connected applications.

Eric Schmitt, Missouri

Founded in 2012 in Joplin, Midwestern Interactive provides their clients with embedded teams of experts. The team of nearly 100 assists clients with strategic planning around software, branding, and digital content. In addition, the team at Midwestern Interactive provides their clients with additional on-the-ground support as they implement their digital strategies.

J. D. Vance, Ohio

Located in Cincinnati since their founding in 2016, Canned Spinach is a custom software development company that helps companies of all sizes make a big impact. From some of the smallest startups to some of the largest Fortune 500 companies, Canned Spinach helps businesses bring their ideas into reality by launching new products and services. They provide clients with web and mobile software development, including design and next-generation technology, such as augmented reality experiences.

Shelley Moore Capito, West Virginia

TMC Technologies is an IT services company focused on helping their clients, both Federal and local, with program and project management, scalable system and software engineering, IT infrastructure design and management, and network and telecom services. TMC Technologies has focused a lot of their IT work in their own backyard, providing IT services for West Virginia companies, especially small business owners looking to bring their company into the digital age.

Cynthia Lummis, Wyoming

BlackFog is a cyberthreat prevention company that uses a unique combination of behavioral analysis and data exfiltration technology to identify, stop, and prevent future data hacks, unauthorized data collection, and more across mobile and web endpoints. Their services protect their clients and their clients' most sensitive data and privacy while also strengthening their regulatory compliance.

APPENDIX B

General Views of the App Association on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence

The App Association represents small business innovators and startups in the software development and high-tech space located across the globe.[21] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, that digital economy is worth more than $1.8 trillion annually and provides over 6.1 million American jobs.[22] App Association members create innovative software and hardware technology solutions and are at the forefront of incorporating artificial intelligence (AI) into their products and processes.

AI is an evolving constellation of technologies that enable computers to simulate elements of human thinking—learning and reasoning among them. An encompassing term, AI entails a range of approaches and technologies, such as machine learning (ML) and deep learning, where an algorithm based on the way neurons and synapses in the brain change due to exposure to new inputs, allowing independent or assisted decision making.

AI-driven algorithmic decision tools and predictive analytics are having, and will continue to have, substantial direct and indirect effects on Americans. Some forms of AI are already in use to improve American consumers' lives today; for example, AI is used to detect financial and identity theft and to protect the communications networks upon which Americans rely against cybersecurity threats.

Moving forward, across use cases and sectors, AI has incredible potential to improve American consumers' lives through faster and better-informed decision making enabled by cutting-edge distributed cloud computing. As an example, healthcare treatments and patient outcomes stand poised to improve disease prevention and conditions, as well as efficiently and effectively treat diseases through automated analysis of X-rays and other medical imaging. AI will also play an essential role in self-driving vehicles and could drastically reduce roadway deaths and injuries. From a governance perspective, AI solutions will derive greater insights from infrastructure and support efficient budgeting decisions.

Today, Americans encounter AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition (we urge consideration of these forms of AI as "narrow" AI). The App Association notes that this "narrow" AI already provides great societal benefit. For example, AI-driven software products and services revolutionized the ability of countless Americans with disabilities to achieve experiences in their lives far closer to the experiences of those without disabilities.

Nonetheless, AI also has the potential to raise a variety of unique considerations for policymakers. The App Association appreciates the efforts to develop a policy approach to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers.

1. Harmonizing and Coordinating Approaches to AI

---

[21] ACT | The App Association, *About,* available at *http://actonline.org/about.*

[22] ACT | The App Association, *State of the U.S. App Economy: 2023, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf*

A wide range of federal, local, and state laws prohibit harmful conduct regardless of whether the use of AI is involved. For example, the Federal Trade Commission (FTC) Act prohibits a wide range of unfair or deceptive acts or practices, and states also have versions of these prohibitions in their statute books. The use of AI does not shield companies from these prohibitions. However, Federal and state agencies alike must approach the applicability of these laws in AI contexts thoughtfully and with great sensitivity to the novel or evolving risks AI systems present. Congress and other policymakers must first understand how existing frameworks apply to activities involving AI to avoid creating sweeping new authorities or agencies that awkwardly or inconsistently overlap with current policy frameworks.

2. Quality Assurance and Oversight

Policy frameworks should utilize risk-based approaches to ensure that the use of AI aligns with any relevant recognized standards of safety, efficacy, and equity. Small software and device companies benefit from understanding the distribution of risk and liability in building, testing, and using AI tools. Policy frameworks addressing liability should ensure the appropriate distribution and mitigation of risk and liability. Specifically, those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should have appropriate incentives to do so.

Some recommended areas of focus include:

- Ensuring AI is safe, efficacious, and equitable.
- Encouraging AI developers to consistently utilize rigorous procedures and enabling them to document their methods and results.
- Encouraging those developing, offering, or testing AI systems intended for consumer use to provide truthful and easy-to-understand representations regarding intended use and risks that would be reasonably understood by those intended, as well as expected, to use the AI solution.

3. Thoughtful Design

Policy frameworks should encourage design of AI systems that are informed by real-world workflows, human-centered design and usability principles, and end-user needs. AI systems should facilitate a transition to changes in the delivery of goods and services that benefit consumers and businesses. The design, development, and success of AI should leverage collaboration and dialogue among users, AI technology developers, and other stakeholders to have all perspectives reflected in AI solutions.

4. Access and Affordability

Policy frameworks should enable products and services that involve AI systems to be accessible and affordable. Significant resources may be required to scale systems. Policymakers should also ensure that developers can build accessibility features into their AI-driven offerings and avoid policies that limit their accessibility options.

5. Bias

The bias inherent in all data, as well as errors, will remain one of the more pressing issues with AI systems that utilize machine learning techniques in particular. Regulatory agencies should examine data provenance and bias issues present in the development and uses of AI solutions to ensure that bias in datasets does not result in harm to users or consumers of products or services involving AI, including through unlawful discrimination.

6. Research and Transparency

Policy frameworks should support and facilitate research and development of AI by prioritizing and providing sufficient funding while also maximizing innovators' and researchers' ability to collect and process data from a wide range of sources. Research on the costs and benefits of transparency in AI should also be a priority and involve collaboration among all affected stakeholders to develop a better understanding of how and under which circumstances transparency mandates would help address risks arising from the use of AI systems.

7. Modernized Privacy and Security Frameworks

The many new AI-driven uses for data, including sensitive personal information, raise privacy questions. They also offer the potential for more powerful and

granular privacy controls for consumers. Accordingly, any policy framework should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Policy frameworks must be scalable and assure that an individual's data is properly protected, while also allowing the flow of information and responsible evolution of AI. A balanced framework should avoid undue barriers to data processing and collection while imposing reasonable data minimization, consent, and consumer rights frameworks.

8. Ethics

The success of AI depends on ethical use. A policy framework must promote many of the existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. Relevant ethical considerations include:

- Applying ethics to each phase of an AI system's life, from design to development to use.
- Maintaining consistency with international conventions on human rights.
- Prioritizing inclusivity such that AI solutions benefit consumers and are developed using data from across socioeconomic, age, gender, geographic origin, and other groupings.
- Reflect that AI tools may reveal extremely sensitive and private information about a user and ensure that laws require the protection of such information.

9. Education

Policy frameworks should support education for the advancement of AI, promote examples that demonstrate the success of AI, and encourage stakeholder engagements to keep frameworks responsive to emerging opportunities and challenges.

- Consumers should be educated as to the use of AI in the service(s) they are using.
- Academic education should include curriculum that will advance the understanding of and ability to use AI solutions.

10. Intellectual Property

The protection of intellectual property (IP) rights is critical to the evolution of AI. In developing approaches and frameworks for AI governance, policymakers should ensure that compliance measures and requirements do not undercut safeguards for IP or trade secrets.

The CHAIR. Thank you, Mr. Reed, and on that last point we will have you expand today or more generally for the record what we need to do about that last point.

I definitely think in the past we have sided too much with the big companies on the patent side and not enough empowerment of the inventors—the smaller companies.

So I want to make sure we get that part right in addition to the—your recommendations. You have made a couple of very good recommendations. Thank you.

I would like to go to a couple of charts here, if we could. One, when we first started working on the privacy law—I am going to direct this to you, Professor Calo—but what got me going was the transfer of wealth to online advertising.

I do not think people really quite understood how much the television, newsprint, radio, magazine, the entire advertising revenue shift, went online. Now we are just talking about the internet.

Could you bring that a little closer, please? Get that up a little closer. So we are now at—oops. We are now at 68 percent.

I do not know if people can see that, but we are now at 68 percent of all spending—two-thirds of all spending, of advertising, has now taken place online with data and information.

So that trend is just going to keep continuing. Now, you and I have had many conversations about the effect of that on the news media having community voices. Our community in Seattle, King Five, or the Seattle Times could not exist if it had misinformation. It just would not—it would not exist. But in the online world you can have misinformation. There is no corrective force for that. But all the revenue has now gone to the online world.

And the second chart describes, I think, a little bit about your testimony that I want to ask a question about and that is the amount of information that is now being derived about you that AI is this capacity to derive sensitive insights.

So that trend that I just described where two-thirds of all advertising revenue—I mean, somebody said data is like the new oil. It is just where everybody is going to go and make the money.

So that is a lot of money already in that shift over that—those years that I mentioned on the chart. But now you are saying they are going to take that information and they are going to derive sensitive information about us.

Ms. Kak said it is the way your voice sounds. You have described it as various features. So could you tell me how protecting us against that in the AI model, why that is so important?

And I just want to point out we are very proud of what the Allen Institute is doing on AI. We think we are the leaders in AI applications. We are very proud of that both in health care, farming, energy.

We have an agreement today between the United States and Canada in principle on the Columbia River Treaty. I think water AI will be a big issue of the future—how do you manage your natural resources to the most effective possible use.

So we are all big on the AI implications in the Pacific Northwest but we are very worried about the capacity to derive sensitive insights and then, as you mentioned, an insurance company or somebody using that information against you.

Could you expound on that, please?

Mr. CALO. Absolutely. I was talking to my sister, who is on the board of the Breast Cancer Alliance, about my testimony and she said, you know, Ryan, just make sure that people know how important it is for AI to be able to spot patterns in medical records to ensure that people get better treatment, for example, for breast cancer, and I agree with that.

And I am also proud of all the work we are doing at the University of Washington and Allen. The problem is that the ability to derive sensitive insights is being used in ways that disadvantage consumers and they are not able to figure out what is going on and fight back.

So, for example——

The CHAIR. Thereby driving up costs?

Mr. CALO. For example, right. I mean, you know, we know why everything costs $9.99. It is because your brain thinks of it as being a little bit further away from $10 than it really is.

But the future we are headed to and even the present is a situation where you are charged exactly as much as you are willing to pay in the moment. Say, I am trying to make dinner for my kids

and I am just desperately trying to find a movie for them to stream that they both can agree on.

If Amazon can figure that out or Apple can figure that out they can charge me more in the moment when I am flustered and frustrated because they can tell.

If that sounds farfetched, Senator, Uber once experimented with whether or not people would be more willing to pay surge pricing when their batteries were really low on their phone because they would be desperate to catch a ride.

Amazon itself has gotten into trouble for beginning to charge returning customers more because they know that they have you in their ecosystem. This is the world of using AI to extract consumer surplus and it is not a good world and it is one that data minimization could help address.

The CHAIR. Thank you.

Senator Wicker.

STATEMENT OF HON. ROGER WICKER,
U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Well, thank you very much, Madam Chair.

Mr. Reed, let me go to you. You have testified before on this topic. Where are most of the jobs created in the United States economy? What size business?

Mr. REED. So small businesses are the single largest source of new business—of new jobs in the United States.

Senator WICKER. OK. And so let us talk about how this—the current situation affects small and medium sized businesses and how legislation would affect them positively or negatively.

Let us pretend I am a small business owner in the state of Washington or the state of Mississippi and I use the Internet to sell products in multiple states. That would be a very typical situation, would it not?

Mr. REED. Yes. In fact, one of the hardest things that I think has been transformative but yet it is hard for legislatures to understand is our smallest members are global actors.

My smallest developers are selling products around the world and are developing a customer base around the world, and in many ways you can think of it this way. Maybe there is 5,000 people in your hometown who want to buy your product but there is 500,000 people who want to buy your product everywhere.

So as a small business the Internet allows you to reach all of those customers. The problem with APRA carving out small business is all of the sudden now a small business that wants to grow from 10,000 customers in the great state of Mississippi to 500,000 customers throughout the United States. Has to comply.

Senator WICKER. So we—the law needs to apply evenly——

Mr. REED. Correct.

Senator WICKER.—to all actors. Let us talk about preemption.

If I am this small businessperson in the state of Washington and Congress passes a new data privacy law but the preemption clause has enumerated exceptions for various reasons. How is that going to affect me?

Mr. REED. Once again, the people who are best equipped to deal with complex compliance regimes are very large companies that hire large numbers of lawyers.

So we really need a compliance regime and a preemption regime that is easy to understand and is applicable. When my businesses do not have a compliance team—heck, they do not even have a compliance officer. It is probably the chief dishwasher is also the chief compliance officer. And I think that is an important thing to understand about small businesses is they do not have teams of lawyers.

Senator WICKER. How about the private—a broad private right of action? How is that going to affect me and my business?

Mr. REED. Well, I think it is interesting that you bring it up. When I testified before you on the same topic we had great discussions about the fact that there may be needs occasionally for private right of action but they should be limited in scope and I think that is more true now than ever before.

If we have a privacy regime that exposes small business and everyone else to individual private right of action from multiple states it sets up small businesses to be the best victim for sue and settle.

Nobody wants to go to war with Microsoft but I can send you, a small business, a pay me now note for $50K. I am going to go to my local small town lawyer, I am going to say, can you fight this?

He is going to say, it is going to be $150,000 to fight it. So you are going to stroke a check and you are going to not pay an employee or not hire someone for $50K.

So we want to avoid a private right of action that leads to the ability for unscrupulous lawyers to make a killing off of sue and settle, particularly in small businesses where the cost of fighting is greater than the cost of the check they are asking for.

Senator WICKER. OK. We are going to run out of time real quick.

But, Mr. Calo, on page 6 of your testimony you say expecting tech companies to comply with a patchwork of laws—and that would be small and large tech companies—a patchwork of laws depending on what state a consumer happens to access their services is unrealistic and wasteful.

I hear people say this, let us pass a nationwide data privacy act. But if a state like California wants to really, really protect even better let us let them do so. Let us give states like that an option out ability. Does that not start the patchwork all over again?

Mr. CALO. Senator, it is an excellent question.

My view is that in a perfect world the Federal Government would set a floor and then the individual states, if they wanted to be more protective of their own residents, would be able to raise that that floor for their own citizens.

In this particular context it is very difficult to deploy these large global systems in ways that differentiate depending on what state you are in.

Senator WICKER. OK. And I am sorry I have to go.

Mr. Reed, that is getting back to the patchwork, is it not? So now you got to comply with two and then who is going to decide which is more protective?

Mr. REED. Absolutely. That is it in a nutshell. Try and figure out what those are.

The CHAIR. I think Mr. Calo—I think Mr. Calo just said it is not realistic to have the patchwork. I think his testimony is quite clear. He says you have to have a Federal preemption.

Mr. REED. [Off mic.]

The CHAIR. Yes, it—I do. I think it does and I think, I think, Mr. Reed, I think your——

Senator WICKER. OK. Well, Madam Chair, since there are not dozens of us but only a couple——

The CHAIR. Senator, we have one of our colleagues who is waiting, Senator Rosen, who actually has coded before so I feel like we need to defer to her.

So Senator Rosen.

STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA

Senator ROSEN. Well, thank you. Writing that computer code it was a great experience, a great living, and I loved every minute of it and now it prepares me for a lot of things I do here today.

So thank you for holding this hearing. These issues are so important. I really appreciate the witnesses.

I am going to talk first a little bit about AI scams because Americans are generating more data online than ever before, and we know with advances in AI, data can be used in many ways depending on the algorithms that are written. And, of course, bad actors are going to use AI to generate more believable scams using the deep fake, cloning, and all the pictures. You have seen it. Everyone has seen it everywhere, and these particularly target our seniors and they target our veterans.

And so I would like to ask each—Ms. Kak and Professor Calo, both of you, how can enacting a Federal data privacy law better protect individuals from these AI-enabled cyber attacks and scams that we know are happening every single day in every community?

Ms. KAK. Thank you, Senator.

Senator ROSEN. Ms. Kak, we will start with you and then we will go to the professor.

Ms. KAK. Thank you, Senator.

It is interesting because when ChatGPT was released and there was all of this excitement about whether we were one step—who knows if it is tomorrow or in 50 years but one step away from these sort of fantastical Terminator like scenarios.

What we were really more concerned about was had we just seen the creation of the most effective spam generator that history had ever seen.

And so I think what is at the heart of these issues is that we are creating these technologies that are moving to market clearly before they are ready for commercial release and they are sort of unleashing these diffuse harms including, as you mentioned, the risk of sort of exacerbating concerns of deceptive and spam content.

To your question on how would a Federal data privacy law sort of nip these kinds of problems in the bud, I think it would do so in a very sort of structural sense.

It would say that there need to be certain rules of the road. There need to be limits on what companies are able to collect, the ways in which they are training their models, so that these companies are not creating inaccurate sort of misleading AI tools which are then being integrated into our most sort of sensitive social domains, whether that is banking or health care or hiring.

So I think the—sort of a final thing I will say on the kind of spam generation point is that we have known for the last decade—we have evidence that garbage in, garbage out.

So when we see these failures we should see them not as output failures but as failures that go back to very crucial data decisions that are made right from the training and development stage of these models all the way through to the output stage and so the privacy risk is——

Senator ROSEN. Thank you. Thank you. I have—Professor Calo, if you could be really brief because I want to get to a question about data ownership—who owns your data and who has a right to your data. So if you could be really brief so I could get that question in I would surely appreciate it.

Mr. CALO. I think that we need to empower Federal regulators such as the Federal Trade Commission to go after all kinds of abuses that involve artificial intelligence including such scams. Investing in the FTC and its expertise is the correct call, in my opinion.

Senator ROSEN. Thank you. I appreciate that because I want to talk about something that everyone talks to me about is data ownership, AI transparency, because Nevadans today, people across this country, do not have the right to access, correct, or delete their data.

Who owns your data? What do they do with it? How do they use it? It matters to people, and so it is impossible for many to even understand, like I said, who holds their data and what they are going to do with it.

So the supply chain of consumer data it is full of loopholes whereas third party resellers they can just sell your data to the highest bidder.

So, Mr. Tiwari, can transparent AI systems exist without strong Federal privacy regulations including consumer control over your own personal data?

Mr. TIWARI. Thank you, Senator, and in short the answer is no.

It is impossible for users to be able to effectively exercise the rights that they have not only over their own data but also their social experiences without knowing what companies are collecting, how that data is being used, and, more importantly, what rights do they have if that harm is occurring in the real world.

We have already in this hearing so far discussed various examples of harms that we have seen occur in the real world but, yet, the actions that regulators and governments have been able to take to limit some of those harms have been constrained by the lack of effective and comprehensive Federal privacy legislation.

Senator ROSEN. Thank you. I appreciate it.

And Madam Chair, I am going to yield back with 8 seconds to go.

The CHAIR. Thank you.

Senator Blackburn.

STATEMENT OF HON. MARSHA BLACKBURN,
U.S. SENATOR FROM TENNESSEE

Senator BLACKBURN. Thank you so much, Madam Chairman. I am so delighted we are doing this hearing today, and as we have talked so many times when I was in the House and our Senate colleague Peter Welch was in the House, we took steps and introduced the first legislation to make businesses take steps to protect the security of our data, to require data breach notifications, and allow the FTC and the state attorneys general to hold companies accountable for violations.

And as Senator Rosen just said, it is so vitally important to know who owns the virtual you—who has that and what are they doing with it and now as we are looking at AI I think Federal privacy legislation is more important than ever because you have got to put that foundational legislation in place in order to be able to legislate to a privacy standard and that is why we are working so carefully on two pieces of legislation—the No Fakes Act that Senator Coons, Klobuchar, Tillis, and I are working on to protect the voice and visual likeness of individuals from unauthorized use by generative AI and then, Madam Chairman, you have mentioned the COPIED Act that you and I are working on, which would require consent to use material with content provenance to train AI systems.

And I want to come to each of you and let us just go down the dias as we are looking at this. We are talking about ways that I would like to hear from you all very quickly—ways that Congress is going to be limited in legislating if we do not have a privacy standard, and then how do we find the balance between that privacy and data security component so that people know they have the firewalls to protect their information and keep it from being used by open source and large language models?

So let us just run down the dais on this.

Mr. CALO. Thank you, Senator.

I was really struck in my research for this hearing by Pew—the Pew Center's research. Their survey suggests that overwhelming percentages of Americans are worried that their data is out there and it is going to be used in ways that is concerning and surprising to them.

I think without passing laws that per Senator Cantwell's remarks define sensitive information to cover not merely already sensitive information like health status but cover the inferences that can be made on top of that data Americans are not going to feel comfortable and safe.

I think that security and privacy go hand in hand. We could sit here and talk about the myriad horrible data breaches that have been occurring across our country. We can talk about ransomware and the way that hospital systems are being shut down.

But ultimately it all boils down to the fact that the American consumer is vulnerable and it needs its government to step in and set some clear rules.

Senator BLACKBURN. Thank you.

Ms. KAK. Thank you, Senator.

I will say that the sort of incentives for irresponsible data surveillance have existed for the last decade. What AI does is it pours gasoline on these incentives.

So, if anything, we have a situation where all of our known privacy and security harms and risks are getting exacerbated.

To the second part of your question, which is what is the connection between privacy and security, I would say those are sort of two sides of the same coin.

So data never collected is data that is never at risk, and data that is deleted after it is no longer needed is also data that is no longer at risk.

So I think having a strong data minimization mandate that puts what we would consider a very basic data hygiene in place is absolutely essential, especially as you are seeing more kind of concerning bad actors use this information in nefarious ways, some of which the legislation you mentioned is going to clamp down on.

Senator BLACKBURN. Thank you.

Mr. TIWARI. Thank you, Senator.

Mozilla is an organization that has hundreds of millions of people that use its products because of its privacy properties. Without providing a consistent standard that allows American companies to compete globally just like they do on innovation but also on privacy, the Congress will be unable to ensure that Americans not only get the privacy rights they deserve but also that American companies can have a high baseline standard with which they can compete with organizations around the world.

Thank you.

Senator BLACKBURN. Thank you.

Mr. REED. And I understand I am over time here, but very quickly, privacy laws should have a data security provision. It is one of our four Ps of privacy.

I think data hygiene is absolutely critical but it is different than a prohibition on processing so let us be careful on how we use the term data hygiene rather than no collection at all.

So let us be smart about how we do that. Thank you.

Senator BLACKBURN. Thank you, Madam Chair.

The CHAIR. Thank you, and thank you for your leadership on the COPIED Act. I think your understanding of creators, artists, and musicians and being able to stick up for them has been really critical. So thank you.

Senator Hickenlooper.

STATEMENT OF HON. JOHN HICKENLOOPER, U.S. SENATOR FROM COLORADO

Senator HICKENLOOPER. Thank you, Madam Chair.

State privacy laws and Federal proposals agree that consumers should have more control, should have control over their personal data including the right to have their data deleted, as has been pointed out.

However, consumers really do not have the time or the expertise to go down and effectively manage all their data online, to fill out the forms to—you know, cookie notices or these lengthy privacy agreements become more of a distraction.

So, Mr. Calo, let us start with you. The American Privacy Rights Act proposes, A, as has been discussed, minimizing personal data collection, but in addition offering consumer-facing controls like data deletion requests and how do these two approaches work in tandem to protect consumers rather than anyone alone?

Mr. CALO. That is a great question. In other contexts where we are trying to protect consumers we do give them information and choices, and we know that privacy preferences are not completely homogeneous.

However, in other contexts not only do we give people choice—for example, how much fat content do they want in their milk—we also place substantive limits like there cannot be so much arsenic.

And so I think that needs to be a combination of both. People should have control over their data and they should be asked before that data is used in a separate context like to set their insurance premiums.

But there also have to be baseline rules because, as you point out, consumers do not have the time or the wherewithal to police the market and protect themselves on their own.

Senator HICKENLOOPER. All right. Good answer.

And, Ms. Kak, you can opine on that as well but I have got another question so let me start with the question.

And you guys have discussed a little bit the advances in generative and traditional AI and how those advances really are fueled by data now.

I mean, we recognize that. But training AI systems cannot be—it really cannot be at the expense of people's privacy and reducing the amount of personal sets of data, as you have all discussed, the notion of minimization does really reduce the likelihood that data privacy and data security harm could happen.

And Senator Blackburn, among all the other bills she listed these issues are covered extensively in various hearings we have had on our subcommittee that she and I chair, Consumer Protection, Product Safety, and Data Security.

So, Ms. Kak, I want to say how would you quantify—how often or what types of quantification do you say when you—when you say how often is the data of consumers unnecessarily exposed within the AI model and do you believe that the strict data minimization requirements can significantly help control this—let us call it data leakage?

Ms. KAK. Senator, there are two parts—two ways in which I will answer that question. The first is to say we do not know and that is sort of part of why we are here today, which is that we do not have basic transparency about whether our data is being used, how it is being protected.

And what we do know is that companies like Meta and Google are sort of at-will changing their terms of service to say, heads up, we are now using your data for AI. At the same time as we are seeing these chatbots routinely leak the personal information they were trained on.

But I think if we did—in the absence of clear data from these companies and a regulatory mandate that allows us to ask them for it I think what we can already see just from the most obvious lapses is that this irresponsible data collection and use is hap-

pening everywhere. It is happening all the time, and I think one of the ways in which the U.S. might benefit from being somewhat of a laggard when it comes to data privacy law is to look at what has not worked elsewhere.

What has not worked is a consent-only based regime. That is why we need accountability in addition to consent. What has worked is that the Brazilian data protection regulator recently banned Meta from using user data to train their AI because they found that there was children's images in the training data and it was being leaked on the other side.

So there is a lot to learn and there is a lot of, I think, a foundation from which to act from.

Senator HICKENLOOPER. Great.

Mr. Tiwari, just quickly—the general data protection regulation—the GDPR—of the European Union has been in effect since 2018, I guess—2019, 2018. Since then it has been amended. They are still sorting it out, I think, in terms of governance structure.

Without a U.S. data privacy law how can we resume—have some leadership on the global stage on these issues?

Mr. TIWARI. Thank you, Senator.

By most counts there are currently at least 140 countries around the world that have a national Federal privacy law. By not having a privacy law the United States of America is not allowing its companies to be able to effectively compete with the companies from these countries and that is because privacy is now a competitive differentiator.

Like I mentioned earlier, people use the Firefox product because they believe in the privacy properties of the Firefox product, and without a baseline of such standards the small and medium companies that we have been talking about will be unable to compete with other small and medium companies around the world.

Senator HICKENLOOPER. Great. Thank you very much. I yield back to the Chair.

The CHAIR. Thank you.

Senator Moran.

STATEMENT OF HON. JERRY MORAN,
U.S. SENATOR FROM KANSAS

Senator MORAN. Chairwoman, thank you very much, and thanks to our panelists. Very important hearing. Thank you for holding it.

Passage of Federal data privacy legislation is long overdue. I chaired the Subcommittee on Data Privacy that Senator Hickenlooper now chairs and Senator Blackburn is the Ranking Member. Senator Blumenthal was the Ranking Member.

We have come so close so many times but never just quite across the finish line and the problems and challenges with our lack of success continue to mount and it gets—I do not know that the issues get more difficult to resolve but we still have not found the will to overcome kind of the differences of the things that each of us think is pretty important.

I reintroduced my Comprehensive Data Privacy—Consumer Data Privacy and Security Act again in this Congress. It gives Americans control over their own data, establishes a single, clear Federal standard for data privacy, and provides for robust enforcement of

data privacy protections that does not lead to frivolous legal actions that would harm small business.

I think these are common sense policies and, again, I think there is a path forward utilizing those and I would, again, say in this hearing as I have said numerous times over the years I am willing to work with any and all to try to find that path forward.

I have a few questions for the panel. I think I will start with you, Mr. Reed.

Important that data privacy requirements, in my view, established by Federal law are shared by consumer-facing entities, service providers, and third parties, all of which may collect or process consumer data.

Exempting segments of this value chain from requirements or enforcement under the data privacy law I think places an unfair burden on consumer-facing entities including particularly small business.

Mr. Reed, is that something you agree with when it comes to data privacy? Regulatory burdens should be shared across the—each entity that collects or processes data?

Mr. REED. I do, but I want to be careful about one thing. I do not want to—I know this sounds weird coming from the business side, so to speak, but I want to be careful that we do not say that shared responsibility becomes everybody touching their nose and saying, I am not it.

So I think the point at which you give your data over, the point at which you have that first contact, whether it is my members through an application or through a store that you visit is the most logical point for the consumer to begin to say, hey, I want my data to be retrieved or I do not want my data used in this way.

So I think, yes, there is shared responsibility across the chain but I do not want a situation where the front person who interacts with the customer can then say, hey, that is down the food chain three third parties from there. So I think it is important.

Senator MORAN. And you avoid that—you avoid that by?

Mr. REED. Well, you avoid that by actually having a clear and concrete conversation, so to speak, with the customer when they provide the data—here is what you are getting in exchange, here is what the rules of the road are—and that is why a Federal comprehensive privacy bill—and we appreciate the bill that you have worked on already on data—moves us in the direction of having consumers nationally have an understanding of what their rights and what our responsibilities are with their data.

So absolutely, but it has to start with an understanding at the first place and then the shared responsibility throughout the chain.

Senator MORAN. One more for you, Mr. Reed.

Nineteen states, I think, is the number that have passed their own data privacy laws. It is a patchwork of state data privacy laws, increasing compliance costs.

One estimate projects compliance costs for business could reach $239 billion annually if Congress does not implement a data privacy law. Incidentally, I came to Congress believing and still believe that government closest to home is better than government far away.

But it seems like I spend a bunch of my time trying to figure out how we take care of a complex situation with 50 different states and 50 different standards. Kansas does not have a data privacy law but borders two states that do.

Mr. REED. Exactly.

Senator MORAN. Would you describe the challenges for small business associated with working in states with different data privacy standards?

Mr. REED. Well, your state is one of the ones in particular that we find most interesting because you literally have businesses in your state that have a primary number of their customers are actually from the bordering state because you have that crossroads that exist.

So for Kansas and Oklahoma you have customers across the border literally every day so having a mixture of these privacy bills. Now, to be clear, a lot of states have some sort of small business carve out but it is different and the definitions are different in every state.

So any business that participates is going to have to figure out who is going to tell them what they do and if that customer walks in and says, my zip code is this, oh, sorry, I have to treat your data this way. If it is this then I have to do it another way.

It is soul crushing for a small business to have to interview each purchaser and ask them what county they live in or what state they live in. So it is a huge burden on small business and, unfortunately, it is one that is really a lot easier for a multinational company to handle.

Senator MORAN. Let me quickly ask Mr. Tiwari and Ms. Kak. it is important for Americans to understand when their data is collected and processed by companies. This belief is reflected in our data privacy legislation which requires covered entities to publish their privacy policies in easy to understand language and to provide easy to use means to exercise their right to control over data.

How can a Federal policy ensure consumers are aware their data is being used even as AI potentially increases the complexity of how consumer data is processed?

Mr. TIWARI. Thank you, Senator.

It is essential for us to recognize that purely relying on consent has proven to be ineffective to protect the privacy of the average consumer.

Technology has now become such a complex endeavor that to expect an average consumer to understand everything that can happen when their data is collected is a burden that they will never be able to meaningfully fulfill and, therefore, any effective Federal privacy legislation must include accountability measures that also place obligations upon these entities for what they cannot do regardless of whether the consumer has consented to that behavior or not.

Only then can consumers be sure that the government is working effectively to predict—to protect their privacy rather than hoping that they understand everything that may happen to that data.

Senator MORAN. It is a sad state of affairs, actually. We cannot understand it well enough to protect ourselves.

Anything to add?

Ms. KAK. Yes. The only thing I would add, Senator, is sort of what do we do as consumers with that information and that is really why transparency is not enough and why proposals like the bipartisan ADPPA and the APRA are so important because they are putting down sort of rules of the rule that apply regardless of consent and what consumers choose.

Senator MORAN. Thank you both.

The CHAIR. Yes. I think Senator—Senator Budd.

STATEMENT OF HON. TED BUDD,
U.S. SENATOR FROM NORTH CAROLINA

Senator BUDD. Thank you, Chair.

So thank you all for being here. Technological leadership is foundational to American dominance in the 21st century.

In this country we innovate, create products and services that consumers want, which increase productivity and it sharpens competition. This spurs a positive cycle of further innovation. The Internet is a perfect example of that.

And one of the factors that differentiates America is it is a regulatory environment that protects public interest and safety while at the same time giving talented entrepreneurs and specialists the space to try new things.

I think that AI should follow this tried and true path.

Mr. Reed—thanks again to all of you for being here. Mr. Reed, thank you for your opening example a few moments back in your opening comments about hog farms. Being from North Carolina I really appreciate that and makes me only wish I had a little more bacon for breakfast. So——

Mr. REED. That was a good call.

Senator BUDD. That is right. Well, in your testimony you talked about the different ways that App Association members are creating and deploying AI tools. In fact, you said that 75 percent of surveyed members report using generative AI.

Do you believe that there is currently a healthy amount of competition in this space?

Mr. REED. Well, I think what has been most amazing is the level of competition against bigger players is profound. The news is always covering Microsoft's moves and Meta's moves and other players' moves but I am telling you right now that we are seeing more moves by small and medium sized companies to use AI in important ways.

And one quick and critical example—if you have got a small construction business in a town, right now to bid on an RFP that gets let it is a lot of nights of coffee and desperate typing on your computer to try to get one RFP out.

But if I can look at all of your RFPs with AI, look at what you do best, what you claim you do best, and help you write that RFP so that instead of filing one you file 10. Maybe you win two bids. Now you hire three people. I used your own data.

A lot of my panelists are talking about using consumer data and sucking in consumer data. What my members are doing with a lot of this is actually using your private data stores to look at what you are doing well and help you improve upon it, and I think when we talk about AI and privacy we have to remember that the ability

to do something like that, simply help you write 10 RFPs, is a huge advantage that AI provides and it is something, frankly, small businesses are doing better than the large businesses right now.

Senator BUDD. I appreciate that example, especially the advantages for small businesses. I read about four newsletters a day on this very topic so I am fascinated with it.

The question, Mr. Reed, is about the FTC's antitrust policy that seems to be focused against vertical integration and we think it may have a chilling effect on your members' ability to develop and roll out new and better AI services.

Even with some of the bigs we see—like, with Open AI, of course, people read news about that every day but Microsoft and Apple not even having a board presence there.

I do not know if that is fear against antitrust legislation or what but we see that there is potentially a chilling effect. Do you having any thoughts on that?

Mr. REED. Yes. Unfortunately, the Federal Trade Commission's proposed rule on Hart-Scott-Rodino is terrible.

I probably should use better words here in the Committee but it really puts small businesses at a huge disadvantage because it essentially establishes a floor for the potential for an acquisition, and what that does for small AI companies that are trying to figure out how to make their way in the world is to seek venture capital venture capitals—venture capital or even your parents they have to believe in your dream and part of that dream is that you can have a huge success.

When venture capitalists are putting money in they are looking at a portfolio and they know nine out of 10 are going to fail. But if the FTC is essentially saying that they are capping at $119 million anybody's success level then that tells the venture capitalists to change the nine companies they are investing in because they cannot dream bigger than $119 million.

We also think that the Hart-Scott-Rodino proposal as put forth violates the Reg Flex Act because they actually did not take into consideration the impact on small and medium sized businesses.

So yes, it has a huge impact on competition for small new AI startups and we are incredibly disappointed and we look forward to seeing if we can convince the FTC to do the right thing and change their way.

Senator BUDD. I appreciate your thoughts on that.

Back to your comments on small business. I do not know if that weighs into your answer on the next question, Mr. Reed, but how should this committee weigh the need for firms to be able to use responsibly collected consumer data with the serious concerns that consumers have about the fact that their sensitive data may be breached or improperly used? How do we look at that as a committee?

Mr. REED. Well, as a committee the first thing to do, which you have heard from everyone about two dozen times, is pass comprehensive privacy reform in a bipartisan way because that gives businesses the rules of the road on how to behave with consumer data.

And figuring out how we balance data hygiene, data minimization, and all those questions are going to be part of the hard work that the Senate has to do on this topic.

But, overall, I would anchor it in the concept of harms—what harm is being done, what is the demonstrable harm, and how do you use the existing law enforcement mechanisms to go after those specific harms.

I think it is a lot easier to empower existing law enforcement action than it is to try to create a new one out of whole cloth and hope it works.

Senator BUDD. I appreciate your thoughts. I thank the panel for being here.

Chairwoman, I yield back.

The CHAIR. Thank you so much.

Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much. Appropriate that we are doing this remotely for a tech hearing.

I wanted to, first of all, talk about the fact that AI, and I have said this many times, quoted David Brooks. He says he has a hard time writing about it because he does not know if it is going to take us to heaven or hell, and I think there are so many potential incredible benefits coming from state of the Mayo Clinic that we are going to see here.

But we have to put some guardrails in place if we are going to realize those benefits and not have them overwhelmed by potential harm, and I know a lot of the companies involved in this agree.

We do have to remember when it comes to privacy these are no longer just little companies in a garage that resisted any rules for too long and whether it is competition policy, children's privacy, that we need to put some guardrails in place and it will be better for everyone.

So I want to start—Professor Calo, your testimony discussed how companies can collect or buy vast amounts of a person's nonsensitive information from what is in their shopping cart to their posts on social media, and use AI to process all that data and make sophisticated inferences about their private health information such as pregnancy status, whatever, with alarming accuracy.

Can you speak to how data minimization can ease the burden on consumers trying to protect their privacy?

Mr. CALO. Thank you, Senator.

Yes, it is a critical issue. So many privacy laws—almost all of them—differentiate between sensitive categories of information such as health status and more less sensitive information, even public information.

But the problem with these AI systems is that they are extremely good at recognizing patterns in large data sets and so they can infer sensitive things from.

And so how would data minimization help? Well, data minimization would, of course, restrict the overall amount of information in the categories for which it could be used.

I think the most effective tool is to define categories of sensitive information to include not just sensitive information itself that is collected from the consumer as sensitive or observed somewhere but also those sensitive inferences that are derived from AI.

I think that is the clearest way. That way you know as a corporation—please.

Senator KLOBUCHAR. OK. Very good. Good answer. Thanks.

Mr. Tiwari, any comments on that, we have demand for data at an all-time high and will comprehensive privacy legislation, perhaps, sort of shape what developers and deployers do to adopt more privacy-preserving systems as they develop things which they are already doing?

Just quickly.

Mr. TIWARI. Thank you, Senator.

We very quickly and sort of very recently acquired an organization called Anonym and what Anonym does is it takes privacy-preserving technologies and within trusted execution environments performs the operations that would take place in large distributed systems in a way that nobody can see the data, not the entity that is giving the data, not Anonym and nor the entity that is using the data in order to carry out, in this case, attribution for advertising.

And we believe that these technologies are showing a path forward that not just minimizes data collection but also showcases that even when data is being processed similar to on device processing what are the ways in which it can be done that minimizes the risk to the average consumer and improves risk and liability for companies. Thank you.

Senator KLOBUCHAR. Thank you.

Ms. Kak, Senator Thune and I have a bill—I think you may be familiar with it—the AI Research, Innovation, and Accountability Act—to increase transparency and accountability for the riskiest nondefense applications of AI.

It directs the Commerce Department to set minimum testing and evaluation standards for AI systems that pose the highest risk such as systems used to manage our electric grid, other critical infrastructure.

It also requires AI deployers to submit regular risk assessments and transparency reports to the Commerce Department that among other things document the source of the AI data used to train employees.

Do you agree that transparency in the datasets used to train commercially available models can do more to protect consumer privacy but also ensure more reliable systems?

Ms. KAK. Absolutely, and, Senator Klobuchar, we are actually seeing some of these big tech companies argue in their policy briefs that it is the training stage that is irrelevant and we should only be focusing on the output stage.

But that could not be further from the truth and it is very clearly in service of their interests alone. So I think we should really double down on both transparency but also testing and evaluation throughout the life cycle of an AI product.

I will also say that companies should not be getting to grade their own homework so the actual metrics that we use for this eval-

uation should be set by regulators. It should be set by public bodies and not the companies themselves.

Senator KLOBUCHAR. OK. Very good. Thank you, all of you. I have a question on voice cloning scams and one on kids' privacy that I will submit on the record to all of you.

So thank you very much.

The CHAIR. Senator Vance.

STATEMENT OF HON. J. D. VANCE,
U.S. SENATOR FROM OHIO

Senator VANCE. Thanks, Madam Chair. Thanks to our four witnesses for being here.

I would direct my questions to Mr. Reed and appreciate in particular your testimony. There is this concern in this building and across Washington that AI poses a number of safety concerns, and I fully admit that there are a number of issues I worry about as AI continues to develop.

In particular, you can imagine a scenario where AI makes these chatbots much more efficient, much more believable, allows predators to prey on children more easily online. That is a real concern and something that I think that we in this committee should be very concerned about, and I know that is a bipartisan worry.

On the flip side of it I also worry that that legitimate concern is justifying some over regulation or some preemptive over regulation attempts that would, frankly, entrench the tech incumbents that we already have and make it actually harder for new entrants to create the innovation that is going to sort of power the next generation of American growth and American job creation.

And I want to just get your reaction to that thought, Mr. Reed, and what you are seeing in your work, and the one additional observation I will make is very often CEOs, especially of larger technology companies that I think already have advantaged positions in AI, will come and talk about the terrible safety dangers of this new technology and how Congress needs to jump up and regulate as quickly as possible, and I cannot help but worry that if we do something under duress from the current incumbents it is going to be to the advantage of those incumbents and not to the advantage of the American consumer.

Mr. REED. Well, thank you for the question and, of course, that is the normal behavior of any company that has significant compliance resources is to look for ways to make sure that they are prepared to comply.

Obviously, they face billion and trillion dollar risks so for them it is viewed through that lens of risk versus opportunity. So completely agree, and that is what is, to a certain degree, trying to shape this environment.

What I have noticed is that AI outside of the context of the large headline news is really empowering the way that small businesses can do activities that they are currently not very good at and do them better.

For example, if you are a small business owner one of the things that you run into all the time is am I buying my—am I buying my inventory at the right time? Am I on 30-day net, 60-day net, or 90-day net?

Every small business owner in your state knows those terms. What I would like to do is I want to use AI to look at my last 3 years of bookkeeping and figure out am I buying the wrong thing? Am I buying at the wrong time? Am I missing my 30-day net and not paying and losing money because that costs me my next customer and that, more importantly, costs me the next person I am going to hire.

So those are the kinds of areas that we need it. I heard one of the other witnesses talk about we need no inferences on sensitive data. I am a little concerned about that as well in the context of what you ask.

I have had the privilege of serving on a Federal advisory committee for HHS for both this and the previous administration and one of the things we talk about a lot is something called social determinants of health, and in the state of Ohio it is really important to figure out do people have access to nutrition, do they have access to the internet, do they have access to telemedicine—all the services that are in there and you need AI to help build inferences about the health and well being of those citizens of your state.

So I think it is whether you are careful to have these blanket no inferences but, rather, talk about the real harms. So agree with you completely on what you said at the beginning, which are the real structural and functional harms that can happen from AI.

But I think we should look through the lens of harms to make the choices that Congress has to make.

Senator VANCE. So with my brief time just one question on who has done data privacy in—one of the benefits of our Federal system, to back up a little bit, is sometimes the states do something that is really smart and, frankly, sometimes they do something that is very stupid, but we can sort of learn from it before projecting a national regulatory regime without any experience.

Who has done this well? Who has done data privacy well?

Mr. REED. I think the structural model that has worked best so far from the states is what is sometimes called the Virginia model but it is Virginia, Colorado, Connecticut, Delaware, Montana, and Oregon have kind of taken that structural model.

If I had any suggestion I think starting with that model as a path forward for the Federal Government is a good idea. It has a lot of broad support.

But what we cannot have is everybody with their own flavor. I do not want 31 flavors of a privacy bill. I want a model that applies to everyone everywhere.

Senator VANCE. Yes. OK. Thank you, and thanks to the rest of witnesses, too. I yield.

The CHAIR. Thank you.

Senator Budd.

Who else is—I think we are waiting for Senator Welch. OK.

Nobody else online? Nobody else? Yes, yes. No, no, I got it.

Senator Schmitt. Senator Schmitt.

STATEMENT OF HON. ERIC SCHMITT,
U.S. SENATOR FROM MISSOURI

Senator SCHMITT. Thank you, Madam Chair.

The CHAIR. Thank you.

Senator SCHMITT. And I want to thank the witnesses for being here today, too.

In my duties as a member of both the Senate Commerce Committee and the Armed Services Committee I have come to realize the significant implications that AI has for the future, not only for our government but the economy and the citizens of this great country.

AI as a power—has the potential to transform many types of commercial applications and is already playing a pivotal role in various aspects of our national security apparatus.

St Louis, Missouri, where I am from, in particular is helping lead that charge through Scale AI and its innovative data annotation and curation systems as well as its advanced model testing and evaluation approach.

Scale AI is partnering with important government entities such as the NGA in St. Louis as well as notable commercial applications like OpenAI to improve AI modeling.

Axios reported this week that U.S. private sector investments in AI outpace every other leading nation, more than doubling investments of our pacing threat China. Members of this committee will speak to the need potentially for overreaching guardrails related to AI.

While I believe targeted measures may be warranted where current gaps in law may exist it is critical that we are not over reactive. Any new laws must not hinder investments in innovation being made by our private sector.

Unfortunately, the approach by the Biden administration and others in this body threatens investments. Monolithic regulatory regimes pushed by this administration pick winners and losers.

AI needs innovation both large and small. It needs innovators both large and small. Only the largest of the companies can comply with sweeping regulations, which is precisely why I believe big tech supports these proposals.

There is an unholy alliance right now between the current administration and big tech to crowd out future competition. Additionally, I fear that the Biden administration's efforts on AI are a backdoor attempt to use regulators to silence their political opponents.

I recently led a letter with Senator McConnell, Senator Thune, and Ranking Member Cruz calling out the efforts by the FCC to now police the content of political advertising through regulation of AI leading up to the 2024 elections.

The goals of the administration to hide in plain sight. They will leave no stone unturned to use big tech and regulations to squash out those that they disagree with.

While I think this hearing provides an important opportunity for us to hear from our witnesses and gain valuable insight into the greater AI and privacy ecosystem, I feel it incumbent upon us to also ask which existing laws can address the fears expressed by many of our colleagues on this committee related to AI.

And as you guys know, AI has dominated a lot of these discussions and one thing that has become increasingly clear is that we have many existing laws in place already that address conflicts involving AI.

For example, it is currently illegal to commit mail fraud. It should not matter whether or not the person uses AI to write the letter or a pen. It is still illegal.

We have seen other countries prematurely attempt to over regulate this technology and it is clear we cannot follow their lead.

So my first question here to Mr. Reed, as Congress debates the need for regulation of AI it is clear we need to focus on the gaps in the system and not create a whole new regime.

With that said, what purely new regulations do you think are needed based on the gaps in our existing regulatory system?

Mr. REED. Thank you very much for the question, and I am going to sound like a broken record but it is a comprehensive privacy bill that clearly defines what are the responsibilities of business on how do we communicate to you and what we are going to do with your data.

Because to take a step back, almost all the questions that arise on this are about customers having an unexpected outcome. You heard earlier from the Chair. She talked about how polling numbers show that most Americans are convinced that something is going to happen with their data that they do not expect or is not—and not in their interest.

That is our fault in business and that is a problem with the regulation because we have different ways in which we are supposed to communicate with customers on what we are supposed to do.

So I think, step one, tell customers what we are going to do, step two, meet those expectations, and to your point, step three, have existing laws that are already on the books—go after us when we do not.

And I think that is a big part of the problem.

Senator SCHMITT. Mr. Tiwari, do you agree with that?

Mr. TIWARI. Absolutely. It is very clear that the benefits of having privacy legislation is something that Americans are already quite familiar with, thanks to laws like HIPAA for health, COPPA for children, that have been in the books for a very long time and have been remarkably effective at preventing some very serious harms.

Comprehensive Federal privacy legislation will go a very long way in ensuring that protection is available to every American.

Senator SCHMITT. Mr. Reed, given the rapid pace of AI innovation, especially among startups and individual developers, can you explain how such a regulation might disproportionately impact, if we were to follow this potentially where some people want to go, disproportionately impacts smaller entities that lack the resources of bigger tech companies?

Mr. REED. Absolutely. I think the issue is that we have seen some calls for things like a Federal agency that would license large language models.

It would not be surprising that the companies that will be able to achieve those licenses will just happen to be companies that state their value in trillions of dollars versus small and medium sized businesses.

So what we see is that a privacy law that essentially cabins off the ability to meet the requirements are so high that no small busi-

ness can ever meet it. If a company is highly vertically integrated and already has all of that customer data then they are at no risk.

They have already gotten permission to use all that data and so, going forward, their answer is, fine by us because we have already got it.

Senator SCHMITT. Right, and I guess to follow up on that then, how would that concentration of power that could even be exacerbated than what we have right now under that kind of regime—how would that affect privacy, competition, consumer choice in the AI industry?

Mr. REED. Well, I think it absolutely affects consumer choice.

And, to be clear, I do not want to sound too negative. We actually need platforms. Platforms are actually really critical for us to build on top of.

So I want to see successful large language models and so I do not want legislation to say big companies cannot build large language models. That is terrible, too.

So the right answer is what you kind of came with at the beginning. Look at the existing law enforcement infrastructure, whether it is the Office of Civil Rights at HHS, as Mr. Tiwari discussed, the Federal Trade Commission's ability to enforce COPPA.

We already have those tools on the books. If we go the other direction and regulate it at this high level then it will be almost impossible for small companies to knock off those incumbent positions.

Senator SCHMITT. Well, I mean, it is sort of my final question then. If we go down this road then could that potentially then give our—an advantage to our adversaries who might develop or adopt a more lenient approach accelerating their own advancements to the detriment of what we are trying to do?

Mr. REED. Of course. The Chairwoman and everyone has recognized that the AI ecosystem is global in place and so our competitiveness is global.

I am very proud of the fact that our members sell products around the world to customers everywhere. I heard mention of Brazil. We actually have great developers in Brazil who are doing amazing things, and what is amazing about that is they depend on the innovation that often comes from the United States to build the next product and the next product that serves a customer base that speaks Portuguese and does not speak English. And, yet, a lot of the innovation came from the platforms here that they build on top of.

So our global competitiveness is absolutely impacted if we restrict the access to the technology that drives us forward.

Senator SCHMITT. Thank you. Thank you, Madam Chair.

The CHAIR. Thank you.

Senator Welch.

STATEMENT OF HON. PETER WELCH,
U.S. SENATOR FROM VERMONT

Senator WELCH. Thank you very much, Madam Chair, and I thank the witnesses.

One of the big concerns that all of us have, really, is meaningful consumer notification and consent and how individual information

is being used, and as I understand it large language models are training on massive data sets scraped from all across the Internet and that can include private and personally identifiable information.

And concerningly to me and, I think, a lot of folks researchers found that ChatGPT could be tricked into divulging training data including user IP addresses, e-mails, and passwords, and software patches are not the solution that we need, in my view.

So it is really the reason that Senator Luján and I introduced the AI CONSENT Act and that would require online platforms to obtain consumers' expressed informed consent before using their personal data for any purpose to train AI.

So I want to ask, Mr. Tiwari, do you believe it is more effective to give consumers the ability to opt in to allow companies to use their data or opt out once the data is already being used?

Mr. TIWARI. Thank you, Senator.

Absolutely yes. The Mozilla Foundation has run campaigns over the last four to five months that have explicitly focused on this specific question, both requiring companies to be transparent about the fact of whether they are using personal data in order to train their models and after that to ensure that users have complete control over this processing, meaning both users should be able to consent for such behavior to take place but also that they should be able to withdraw this consent whenever they like and opt out of this processing.

We believe that the risks that exist from the leakage of such private information will drastically reduce if users are given an ability to both understand what their data is being used for and then to make a choice of whether they would like it to be used in that way.

Senator WELCH. OK. Thank you.

Another issue here is small business. They do not have, obviously, the resources, the infrastructure, that big businesses have. Yet, consumer data can be lost or appropriated through that source.

But we do not want to impose huge expenses on small business that they just cannot meet—the local retail florist, let us say. So but we want to protect people's privacy.

So let me just ask, Mr. Calo, what would be a good way to deal with this? I am thinking about either a pilot program or the capacity of the Federal Government to provide sort of a punch list of things that can be done in—to assist small businesses so they do not have to do something that is not within their capacity to do. They want to sell flowers. They do not want to become IT experts.

So perhaps you could tell us how we could protect people's privacy in a way that does not burden small business?

Mr. CALO. What a great question. I mean, it is true that small businesses do not have the capacity to comply at this—with the same sorts of requirements at the same level as large businesses.

A few years ago the Tech Policy Lab at the University of Washington we hosted the "Start With Security" series by the Federal Trade Commission where the FTC was saying, look, it is going to be unfair and deceptive. You do not have adequate security that is proportionate to how much data you have.

But rather than just sort of throw that out there they went on a tour around all the innovation centers. They came, of course, to Seattle but also to San Francisco and elsewhere and they invited smaller companies to talk about the FTC's own expectations.

The more we can do to help scaffold government expectations for smaller businesses the better off we will be. But I agree that you do need to have a tiered system because Google and Meta and Amazon and others have the capacity to comply with far more rigorous detailed rules than do small businesses.

Senator WELCH. Thank you.

I want to ask Ms. Kak this question. Senator Bennet and I have introduced the Digital Commission—the Digital Platform Commission Act, and what it would do is establish an independent Federal commission to regulate digital platforms and that would include on key issues like AI and privacy concerns.

And our theory, essentially, is that the Congress simply cannot keep up with everything that is happening and we cannot address everything in a one-off piece of legislation. There has to be a governmental agency that is properly staffed and resourced to keep up with this.

We have done this in the past when we started the Securities and Exchange Commission, when we started the Federal Aviation Authority, when we did the Interstate Commerce Commission.

Give me your thoughts on just the concept of a digital platform commission as having that responsibility in an ongoing basis.

Ms. KAK. Thank you, Senator, for your leadership on this issue.

In general we do think that independent regulation and sort of resourcing our enforcers is—should be a top priority. What I will say, though, is that I do think that existing enforcement agencies like the FTC have been working on these issues for decades now.

They have the capacity. They have the kind of technical expertise. What the moment needs is for these agencies to be much better resourced so that they can meet the moment and for laws like the APRA and the bipartisan ADPPA which empower them to then enforce clear privacy standards.

Senator WELCH. All right. Thank you very much. I yield back.

The CHAIR. Senator Thune.

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Madam Chair, for holding today's hearing.

It is my view that this committee, which has expansive jurisdiction over technology issues, should play a significant role in understanding how the most recent developments in AI will impact society and existing law and, ultimately, is my belief that this will include developing a thoughtful risk-based legislative framework that seeks to address the impacts of AI which is why I have introduced the AI Research, Innovation, and Accountability Act last year with Senators Klobuchar, Wicker, Hickenlooper, Capito, Luján, Loomis—Lummis, I should say, and Baldwin.

The bill establishes a framework to bolster innovation while bringing greater transparency, accountability, and security to the development and operation of the highest impact applications of AI.

Through this legislation basic safety and security guardrails are established for the highest risk applications of AI without requiring a burdensome audit or stamp of approval from the government, and it is my hope the Committee will advance the legislation soon.

Mr. Reed, there are several proposals out there calling for new AI oversight agency, a licensing regime that would require the government to approve certain AI systems before they could be deployed.

The framework that I just mentioned and that we have been working on with members of this committee would take a more pragmatic approach, in my view, arguing instead that a risk-based compliance and assessment process would provide the necessary oversight while also allowing AI developers and research to innovate more quickly.

In your view how would a licensing regime impact the innovation ecosystem in the U.S.?

Mr. REED. Well, as I touched on earlier, I think licensing regime always leads to a situation where those with the power and the time and the number of lawyers to go through the process of meeting that licensing requirement are the ones who win at the table rather than those that have the best technology or the best ideas.

So I am always concerned about a licensing regime that is the only door into success. We know how that works. You end up with three, four, maybe five competitors and they settle into a nice multiyear program.

I think beyond that I want to say that your work on the risk-based framework is a great idea but I am always hesitant because I know that we need comprehensive privacy legislation.

It has been very hard as people come forth with these great ideas that offer really good alternatives but then will leave out a piece.

Without comprehensive privacy legislation what ends up happening is we have a patchwork and that patchwork costs us.

You made one other critical point that I think is vital, and I have heard it from my fellow panelists. There is, in fact, already existing government expertise.

I have had the honor to work with the Federal Drug Administration—the FDA—and its Center for Excellence, and I would say that they have incredible leadership already on understanding AI frameworks, their development internally about how do I get approval for software as a medical device that includes AI and how do I deal with the difference between black box AI and how do I deal with transparency.

The FDA has been working on this for years. So I think my worry about standing up a new Federal agency when we already have expertise on these topics within existing agencies and I am going to agree with Ms. Kak to say that we need to make sure that we have plenty of resources for them to enforce existing laws.

If you have got a problem in health, OCR. If you have got housing we have got DOJ. You already have mechanisms. You already have harms-based, risk-based assessments that can be done by existing government agencies. It is a lot better to stand up—than standing up a single agency.

And my last point on that is very simple. Anyone who has ever run a business knows that hiring and growing a business while hir-

ing is one of the hardest things. You would be growing and hiring a business inside of the government called a whole new agency while at the same time that everything is changing.

Let us let the experts in each area do their work rather than trying to build out while the plane is already in the air.

Senator THUNE. Yes. And to be clear, we do not call for any kind of a bureaucracy or agency.

Mr. REED. Exactly. Exactly.

Senator THUNE. In fact, that is the—the framework in our bill does not allow for that.

Mr. REED. We thank you for that.

Senator THUNE. That is why we want it to be a light touch approach.

On the privacy issue is it your view that we are better served by having one national standard?

Mr. REED. Absolutely.

Senator THUNE. Yes. OK. And how about the Federal privacy law including a private right of action? What is the practical effect of a provision like that on small businesses and startups?

Mr. REED. The reality is that in order to achieve a bipartisan legislation it is likely that we are going to have to give some consideration to a private right of action.

I think what has to happen is that if Congress considers putting a private right of action in place it needs to ensure that it has numerous backstops to make sure that it does not become an opportunity for kind of ludicrous sue and settle.

We saw that—we have seen that where small businesses will get a letter saying you are using a patent in a fax machine. You owe me $50,000. Pay me. And the cost of fighting that ludicrous suit is greater than the $50,000 you send.

I do not want our privacy laws with a private right of action to lead to one state being kind of the breeding ground for hilarious yet economically untenable action against small and medium sized businesses, because we are the best victims in this.

We have just enough money to pay you but not enough money to fight you.

Senator THUNE. All right.

Madam Chair, my time has expired. I have a question I would direct to Dr. Calo but I will submit it for the record having to do with——

The CHAIR. Go ahead.

Senator THUNE. Well, let me just say that——

The CHAIR. Or whatever you want to do.

Senator THUNE. Well, I just—let me just—very quickly, I see transparencies I mentioned as the key to ensuring that both developers and deployers of AI systems are accountable to the consumers and businesses they serve.

But could you expound just briefly on what constitutes a deployer versus a developer as well as explain how obligations for developers and deployers differ when it comes to transparency and accountability?

Mr. CALO. Yes. I mean, technology generally has a problem of many hands and so you have these foundational models and then you have APIs upon which things are built.

And so effective legislation makes it clear what the respective responsibilities of each of these parties are. For me, personally, speaking on my own behalf, my concern enters into it when whoever it is in the ecosystem is leveraging the tool in a way that harms consumers and tries to extract from them.

So maybe that is the platform but maybe it is somebody using the tools of the platform.

Senator THUNE. All right. Madam Chair, thank you.

The CHAIR. Thank you.

I would actually like to follow up on—and I was going to anyway so it was a good lead in. I want to thank Senator Thune for his leadership because he—not just on data security but on privacy and now on your proposal as it relates to AI. Very good concepts there that we should continue to work on and, hopefully, we will get to a markup soon.

But this notion—this data that came out by the Department of Justice that it had dismantled a Russian bot farm intended to sow discord in the United States and that the AI—the Russians created scores of fictitious profiles and then generated these posts.

And so I am just—I am trying to—you were talking about this ecosystem that is created and now here we have bots who are just exploding with information because we have given them so much data.

You can say it came from the social media platform, that they collected it, and then that information got scraped and then the information got to the bots and then the bots put it on this accelerant and a bad actor can use it against us.

So why is this so important to now have a tool to fight against this? Because the bot system is out of control but the AI accelerant on the bot system makes it an imperative.

Mr. CALO. I can only agree with you, Senator.

Obviously, misinformation and propaganda are not new but the ability of adversaries of all kinds, domestic and foreign, to create plausible looking and very damaging misinformation campaigns has become quite acute.

I mean, I will just use one example. As you know, the Center for an Informed Public studies misinformation and disinformation. One example is that someone created a deep fake that was not real—fictitious—that gave the appearance that there had been a bomb go off at the Pentagon, which was so concerning to people that it actually caused a dip in the stock market until people figured out that it was not real.

The ability to create a seemingly real catastrophic event is very, very dangerous but you are talking to something even more basic which is that AI makes it possible to generate much, much more disinformation and have it appear different from one another—different media, different phrasing, and everything else.

It is deeply, deeply concerning. I think there are ways in which a privacy law could help actually but the problem of disinformation and misinformation probably is broader still.

The CHAIR. So what do we do about the bots from a regulatory perspective?

Mr. CALO. Yes, that is hard. I mean, so states like California have a bot disclosure act. It requires that if you are operating a bot

in certain ways, commercial and electioneering, that you have to identify yourself as fake.

The problem, of course, is that Russian disinformers are not going to comply with our laws and so I think part of the response has to be political and economic.

It is one of the main reasons that the Federal Government needs to get involved because it is not something the states can address. States cannot find global consensus around sanctioning bad acting around information.

But I think that placing responsibility on the platforms to do as much as possible since they have control over their own platforms to identify and disincentivize this kind of misinformation that is automated is also really key.

The CHAIR. Thank you.

Well, I think that concludes our hearing. I know it is a very busy morning for everybody. The record will remain open for two weeks and we ask members to submit their questions for the record by July 18.

I want to thank the witnesses, all of you. A very informative panel. We appreciate you answering these questions and helping us move forward on important privacy and AI legislation.

We are adjourned.

[Whereupon, at 12:01 p.m., the hearing was adjourned.]

A P P E N D I X

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

Executive Summary

The Center for AI Policy (CAIP) commends the Senate for focusing on the critical intersection between AI and privacy. CAIP strongly supports the call for federal privacy legislation to resolve the existing patchwork of state legislation. Specifically, CAIP agrees with the proposal for federal legislation that combines informed consent and privacy by design and applies to businesses of all sizes. Such a model would best protect Americans against misuse of their data and clarify the regulatory environment for businesses.

CAIP also agrees that existing agencies will need additional resources to enforce privacy legislation and track AI-related issues relevant to their agency. Finally, CAIP commends Senators Welch, Thune, and Klobuchar for considering a new AI oversight agency and minimum evaluations standards.

Federal privacy legislation

The US needs comprehensive federal privacy legislation - both to better protect consumers and to clarify requirements for business. The existing patchwork of state legislation is difficult for businesses, particularly smaller firms, to navigate and provides inconsistent protections to US consumers. Moreover, as privacy grows increasingly valuable to consumers, the US's ongoing lack of privacy legislation sends a negative signal about US businesses and makes them less competitive in the global market.

CAIP agrees with Ms. Kak and Mr. Tiwari that a consent mechanism is insufficient to fully protect consumers, and that it should be coupled with minimum requirements for privacy. The burden should not be entirely on the consumer to navigate the complex implications of disclosing their

data. These minimum requirements should clearly define the responsibilities of businesses and be accompanied by tangible consequences to deviation. This legislation should include small businesses, which are particularly affected by the administrative burden from inconsistent state legislation.

Resources

CAIP agrees with the witnesses that existing federal agencies must be augmented with privacy and AI-focused resources. These agencies will need additional capacity to focus on privacy and AI risks relevant to their agency as the technology rapidly advances. For example, the Department of Justice should have additional resources to monitor and minimize privacy violations associated with algorithms used to approve housing. CAIP recommends that a taxonomy of privacy and AI-related risks is developed, identifying topics like housing, education, consumer protection, and that specific agencies are identified as the lead on each risk to ensure clear accountability.

Proposed AI agency and minimum standards

CAIP strongly commends Senators Thune and Welch for considering a dedicated AI agency. While existing agencies should focus on AI risks specific to their agency, without a central coordinating agency, there is a risk of duplication or, worse, that certain AI-specific risks are not addressed. Moreover, CAIP also supports Senator Klobuchar's consideration of minimum testing and evaluation standards for AI systems that pose the highest risk to critical infrastructure.

Conclusion

To conclude, CAIP supports the call for federal privacy legislation that has minimum requirements and consent mechanisms. Such legislation should encompass all businesses so America's entire private sector can benefit from a clarified regulatory environment. Finally, CAIP commends the consideration of a dedicated AI agency and minimum testing for the highest risk systems.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO RYAN CALO

Targeted Pricing

We have seen more and more examples of how AI can exacerbate existing harms online. By automating processes that would be too labor intensive for humans to accomplish alone, AI can enable increasingly personalized targeting. This can be used by bad actors for fraud, but also by companies for advertising and even personalized pricing.

Mozilla and Consumers International recently found that the dating app Tinder used dozens of variables to adjust pricing for its members, with U.S. users paying between $4.99 to $26.99 for the exact same service. Older individuals tended to receive higher prices, highlighting the danger of opaque pricing algorithms to discriminate.

Question 1. Can you speak to the way these harms will increase if we do not put limitations on data collection and use?

Answer. Thank you for your excellent questions, Senator, and for your longstanding leadership on these issues. In 1999, law professors Jon Hanson and Douglas Kysar coined the term "market manipulation" to refer to the ways companies profit off of the cognitive limitations of their consumers.[1] One of their examples involved the use of 9s instead of 10s to induce so-called price-blindness: everything costs $9.99 because it looks farther away from $10.00 than one cent.

Today's companies are not satisfied with such little tricks. They want to use what they know about consumers—plus the power of design—to charge each consumer as much as they are willing to pay—what economist call our "reservation price."[2] Examples include charging consumers higher prices once they become habitual users of the service, as Amazon did,[3] or experimenting with whether consumers might be more willing to pay Uber surge pricing when their battery is low for fear of being stranded.[4] This practice has become prevalent enough that the Federal Trade Commission recently launched an inquiry into "surveillance pricing."[5]

Most consumers would be surprised to learn that companies are studying their every move in order to charge them as much as possible. The phenomenon will only get worse as artificial intelligence makes targeted pricing even more prevalent and sophisticated. Limitations on data collection and use would interfere with the capability of companies to use what they know about consumers to extract more profit.

Deepfake Abuses with Generative AI

A recent study by researchers with Google's DeepMind examined how generative AI is currently being misused and found that the most prevalent form of misuse is impersonating other individuals by manipulating human likenesses—commonly known as deepfakes.

I've heard from my own constituents about scams and fraud using deepfakes, including romance scams that take a celebrity's likeness, manipulate it to personalize a message to an unsuspecting—often elderly—individual, and then request or demand money. AI can be a tool for bad actors to target specific individuals.

Question 1. How can a strong privacy law help prevent these scams before they start?

Answer. The artificial intelligence behind deepfakes requires an enormous amount of training data. Sources of this data includes what is available online, which incentivizes companies to scrape every corner of the internet, as well as the company's own internal data, which incentivizes them to collect as much data as possible and store it indefinitely. A strong privacy law could help ensure that consumer data is not repurposed for nefarious ends.

Question 2. How can we ensure that bad actors using generative AI tools are held accountable?

Answer. Congress can and should pass laws that penalize certain common, harmful uses of generative AI—such as political deepfakes and non-consensual pornography. But it is often hard to identify or reach perpetrators in time. Congress should also set expectations that companies providing generative AI tools to the public maintain adequate safeguards and respond meaningfully to complaints.

---

[1] Jon D. Hanson & Douglas A. Kysar, Taking Behavioralism Seriously: Some Evidence of Market Manipulation, 112 Harv. L. Rev. 1420 (1999).

[2] Ryan Calo, Digital Market Manipulation, 82 Geo. Wash. L. Rev. 995 (2014).

[3] Jonathan L. Zittrain, The Future of the Internet—and How to Stop It (2008).

[4] Ryan Calo & Alex Rosenblat, The Taking Economy, 117 Colum. L. Rev. 1623 (2017).

[5] See *https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-issues-orders-eight-companies-seeking-information-surveillance-pricing.*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO RYAN CALO

In your hearing testimony, while discussing how AI is exacerbating the problems of misinformation and disinformation, you stated "I think there are ways in which a privacy law could help, but the problem of misinformation and disinformation is broader still."

Question 1. Can you elaborate on this statement and describe what concrete policy steps (both by the public sector and/or by non-public entities) you believe are needed to mitigate the risks of digital disinformation and misinformation?

Answer. Thank you for this thoughtful question. I see two promising policy directions to mitigated disinformation. The first involves disincentivizing disinformation at the source. There are different reasons that individuals and groups engage in disinformation. A surprising volume of disinformation is motivated by a desire to reach gullible or vulnerable audiences and sell them questionable goods and services.[6] The government should penalize this strategy. Other disinformation originates abroad and aims to undermine American democracy. Here, political and economic pressure may be more effective than domestic laws.

The second strategy involves expecting more from the platforms where disinformation originates and spreads. Federal law shields social media from liability for most categories of disinformation. But government can still act. Requiring companies to identify, report on, and commit resources to mitigate disinformation on their platform is not the same as treating the platform as the publisher of this content—which is what the Telecommunications Act of 1996 actually forbids via Section 230.[7]

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TED CRUZ TO RYAN CALO

Take It Down Act

In my opening statement, I referenced how artificial intelligence (AI) can be used for nefarious purposes and how Congress should pursue targeted, tailored solutions that address specific harms or issues. It's why Sen. Klobuchar and I introduced the Take It Down Act, which targets bad actors who use AI to create and publish fake, lifelike images of real people—oftentimes teenage girls—in sexually explicit situations. It also gives recourse for victims to get the images taken down.

Question 1. Do you support the policy in the Take It Down Act and agree that Congress should act to stop the proliferation of revenge porn, including deepfake pornographic images of adults and children?

Answer. In a word, yes. I had occasion to watch your June 26, 2024 field hearing. Thank you and Senator Klobuchar for your efforts on behalf of victims. The harms of deepfakes fall disproportionately upon women and vulnerable populations, and not enough is being done to address these harms. The subject matter experts with whom I spoke thought the Take It Down Act could do much good. It would perhaps be wise to (1) define covered platforms more broadly to include websites that also create and curate content; (2) add a provision deterring bad faith complaints; and (3) require takedown within a reasonable time-frame rather than 48 hours.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO AMBA KAK

Data Minimization

We know that LLMs are trained on vast quantities of data. We also know that data leakage—when a large language model accidentally reveals sensitive information, such as personal details of an individual—is occurring. And we know that LLMs can be attacked by bad actors to extract sensitive and confidential data.

Both scenarios become more concerning when LLMs are trained on private data.

Question 1. How would a strong data minimization requirement ensure that training data is scrubbed to remove confidential or sensitive information before it is used to train an LLM?

Answer. A strong data minimization requirement would mean that AI developers would need to design systems in ways that mitigate the risks of these harms—mandating that sensitive or confidential data must only be included where it is strictly

[6] See *https://chequeado.com/investigaciones/how-disinformation-makes-money.*
[7] 47 U.S.C. § 230(c)(1) (1996).

necessary. Moreover, given that the current state of LLM technology cannot guarantee against such unexpected (and routine) leakages in the output phase, a data minimization mandate would guide developers against training models on such sensitive data, or prompt them not to release these systems for public use until such privacy standards were met.

Question 2. How can we allow individuals to have control over their data after it is used to train an LLM?

Answer. Data rights are a crucial complement to the proactive obligations of data minimization, as they empower individuals to ascertain the nature and scale of commercial surveillance, and to act on such information to correct, order deletion, or otherwise seek redress if they believe any other obligations owed to them under the legislation have not been fulfilled.

Currently, the only constraint on usage of any consumer data for training of proprietary models comes from the terms of service of those products, which can be changed at will, as Google and Meta recently did. Notable too that while European users were alerted by Meta that it would use publicly available posts to train its AI, American users received no such notification.

With a comprehensive data privacy law, these individuals would have, at minimum, the ability to demand transparency around the use of their data. Individuals should also have a broad right to opt out of algorithmic decision-making that comprises "consequential decisions"—defined as decisions, including ads, that may impact an individual's equal access to housing, employment, healthcare, and so on. Such algorithmic decision-making is ubiquitous today, with limited oversight.

Overcollection of Data Favors Big Companies

The current model of developing AI systems depends on immense data collection, which lends an outsized advantage to a few companies. Without Federal standards, industry has no baseline standard to follow on data collection.

Question 1. How does Federal privacy legislation even the playing field so that companies beyond the largest ones are able to develop new AI systems?

Answer. As it stands today, there is no AI without Big Tech. These firms already control the resources needed to play this game of scale—compute infrastructure, persistent data collection, and access to the consumer. Currently, the largest consumer technology companies such as Google, Microsoft, and Amazon dominate access to such compute resources (and other companies, as a rule, depend on them for these resources).[1] This is closely related to these companies' pre-existing data advantage, which enables them to collect and store large amounts of good-quality data about billions of people via their vast market penetration.

Data minimization rules could meaningfully constrain the consolidation of this data advantage and in doing so it will contribute to a more level playing so that we see innovation by the many, not the few. While some make the disingenuous claim that data privacy law will hurt competition and smaller players, the reality is the opposite. Proportionality requirements can and have been built into data privacy proposals, including APRA and the bipartisan ADPPA so a small tech business is not subject to the same compliance burden as the largest players. More fundamentally—Big Tech has long tried to position privacy as meaning that our data is safest with them even as they extract, combine, and profile our data without limits and often against the public best interest. This is deceptive and data minimization rules actually level the playing field by hitting at first party not just third party surveillance.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO AMBA KAK

Question 1. What does your research show on how AI companies' use of publicly available data to train and fine-tune their AI models is impacting the creative sectors—including but not limited to independent artists, authors, journalists and musicians?

Answer. While we don't currently focus on the impact of AI on the creative sectors, the concerns here follow the same non-transparent and often extractive dynamics we're seeing more broadly. For example, widespread non-transparency on how AI systems are being trained, extractive practices of using creative work to train AI without consent, or where consent has been obtained by large media publishers via agreements with AI companies, workers have raised ethical and economic con-

[1] Jai Vipra and Sarah Myers West, "Computational Power and AI," AI Now Institute, September 27, 2023, *https://ainowinstitute.org/publication/policy/compute-and-ai.*

cerns about the impacts of the wholesale transfer of their work to AI companies. The broader concern for workers in the creative industry but also more generally is a gradual devaluation of human generated work, leading to reduce opportunities for income and a broader degradation of the value of human labor and creativity.

Question 2. What rights does the AI Now Institute believe all individuals should have with respect to the use of their public data to train AI?

Answer. Data rights are a crucial complement to the proactive obligations of data minimization, as they empower individuals to ascertain the nature and scale of commercial surveillance, and to act on such information to correct, order deletion, or otherwise seek redress if they believe any other obligations owed to them under the legislation have not been fulfilled.

Currently, the only constraint on usage of any consumer data for training of proprietary models comes from the terms of service of those products, which can be changed at will, as Google and Meta recently did. Notable too that while European users were alerted by Meta that it would use publicly available posts to train its AI, American users received no such notification.

With a comprehensive data privacy law, these individuals would have, at minimum, the ability to demand transparency around the use of their data. Individuals should also have a broad right to opt out of algorithmic decision-making that comprises "consequential decisions"—defined as decisions, including ads, that may impact an individual's equal access to housing, employment, healthcare, and so on. Such algorithmic decision-making is ubiquitous today, with limited oversight.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RAPHAEL WARNOCK TO AMBA KAK

Civil Rights and Antidiscrimination

In your written testimony, you describe how AI can "entrench and embed historical inequities in sensitive social domains like healthcare, hiring, education, housing, and criminal justice."[2] Some Federal agencies have already taken action against online platforms for violating Federal antidiscrimination laws.[3]

Question 1. In what ways do existing Federal antidiscrimination laws fail to adequately protect consumers against online discrimination?

Question 2. In your view, are Federal agencies adequately enforcing existing antidiscrimination laws against companies using AI tools? Are there additional steps that Federal agencies should take to enforce existing laws?

Question 3. In establishing new antidiscrimination provisions in a Federal data privacy law, what specific provisions should Congress consider, and what are the key lessons from state-level and international regulations on similar topics?

Answered 1, 2, and 3 together. Data privacy law can provide a crucial remedy to counter data-driven discrimination at the hands of AI tools, and should be viewed as an essential complement to, rather than a substitute for, Federal antidiscrimination protections. For one, using people's personal information to unfairly discriminate against them is one of the clearest cases of abuses of data and therefore falls squarely within scope for data privacy laws. Moreover, in an age where decisions impacting people's access to key opportunities and benefits are increasingly being outsourced to algorithmic software, specific protections that reflect this contemporary context and a tailored enforcement regime will ensure that these harms are addressed comprehensively.

Given rampant opacity in the way AI systems are designed, provisions protecting against such algorithmic discrimination must be formulated to avoid parties being able to shift responsibility to inscrutable machine-based decisions, making sure that the burden of proof to show that systems are *not* discriminatory is on the party that operates the AI system. Such a legal mandate will have a ripple effect in terms of encouraging greater explainability and transparency in the way that firms design and use AI systems for decision making.

Public Understanding of AI and Transparency

Pew Research recently reported that "only three-in-ten U.S. adults can correctly identify all six uses of AI asked about in the survey" and "44 percent think they

---

[2] The Need to Protect Americans' Privacy and the AI Accelerant: Hearing Before the Senate Committee on Commerce, Science, and Transportation (Statement of Amba Kak) at 13–14.

[3] Ariana Tobin and Ava Kofman, *Facebook Finally Agrees to Eliminate Tool That Enabled Discriminatory Advertising,* ProPublica (Jun. 22, 2022), *https://www.propublica.org/article/facebook-doj-advertising-discrimination-settlement.*

do not regularly interact with AI."[4] These numbers underscore the limited public understanding of how often AI is currently used, much less how consumer data may be used to train AI models.

Question 1. In crafting consumer consent and notice provisions, how should Congress best ensure that any information provided to consumers is comprehensible?

Answer. While a data privacy law should not rely on transparency and consent given the significant information and power asymmetries between firms and their consumers, robust transparency remains a key part of the privacy toolkit—especially to uncover where privacy harms might be taking place in the first place. The FTC's updated guidance on the "clear and conspicuous" standard[5] is a useful guide when formulating such a transparency standard. It emphasizes that all disclosures related to AI should be "unavoidable" when using an electronic medium and easily understandable by ordinary consumers. This means that surreptitiously changing terms of service to allow for changed or new uses of personal data or burying disclosures in legalese or behind hyperlinks would likely not meet this standard. Moreover, it requires firms to be creative and proactive about inviting consumer attention to the substance of the disclosure rather than allowing them to comply with a checkbox form of compliance.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TED CRUZ TO AMBA KAK

Take It Down Act

In my opening statement, I referenced how artificial intelligence (AI) can be used for nefarious purposes and how Congress should pursue targeted, tailored solutions that address specific harms or issues. It's why Sen. Klobuchar and I introduced the Take It Down Act, which targets bad actors who use AI to create and publish fake, lifelike images of real people—oftentimes teenage girls—in sexually explicit situations. It also gives recourse for victims to get the images taken down.

Question 1. Do you support the policy in the Take It Down Act and agree that Congress should act to stop the proliferation of revenge porn, including deepfake pornographic images of adults and children?

Answer. We support Congress taking a strong, clear stance penalizing those who distribute and profit from such egregious, harmful uses of AI, and commend Sens. Cruz and Klobuchar's leadership on this issue. These targeted interventions should also be complemented by foundational comprehensive data privacy laws that tackle the incentives for unrestrained surveillance of personal information that is at the root cause of these and other malpractices.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. SHELLEY MOORE CAPITO TO AMBA KAK

Question 1. We know that it is frighteningly easy for minors to bypass website age verification as they can just pick any date over age 21 and be able to access websites or apps. What is the best solution to verify a user's age without infringing on their privacy?

Answer. While this is not a specific area of research for us, we wholeheartedly support formulating approaches to age verification online with privacy as a core guiding principle. This will ensure that any systems put in place are not only robust and secure, but designed with privacy safeguards built in from the start, for *e.g.,* minimizing the personal information that is required or preferring decentralized and "zero-knowledge" approaches. In addition, in this case, we view privacy and competition concerns are two sides of the same coin—enabling Big Tech platforms to require more authentication from users further legitimizes the aggregation of personal information and government ID data across databases, sedimenting their position as gatekeepers of content online in ways that could hurt both privacy and competition.

---

[4] Brian Kennedy, Alec Tyson, and Emily Saks, *Public Awareness of Artificial Intelligence in Everyday Activities,* Pew Research Center (Feb. 15, 2023), *https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities.*

[5] *https://www.federalregister.gov/documents/2023/07/26/2023-14795/guides-concerning-the-use-of-endorsements-and-testimonials-in-advertising*

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO UDBHAV TIWARI

Lack of a Federal Privacy Law is a Global Disadvantage

137 out of 194 countries have national data privacy laws. In many cases, these laws serve as the foundation for countries to develop regulations on AI.

Question 1. How has the United States' lack of a Federal privacy law hindered our global technology advantage?

Answer. The United States' lack of a Federal privacy law has significantly hindered our global technology advantage in several key ways. Firstly, the absence of a unified national standard creates a fragmented regulatory environment, forcing companies to navigate a patchwork of state laws. This not only increases compliance costs but also benefits incumbent films that can afford these bureaucratic expenses, thereby stifling innovation from smaller entities. While Mozilla *supports strong state laws,* we believe that support is not mutually exclusive to the need for a strong Federal standard, *which we have long advocated for.*

Moreover, without clear and robust privacy laws, U.S. companies face lengthy and costly court battles over data collection practices. This legal uncertainty hampers the ability of businesses to develop and deploy AI technologies confidently. For instance, many data collection practices necessary for training AI models are now mired in legal disputes, which may ultimately lead to deleterious effects on innovation, investment, and technological progress. The lack of a national standard leaves companies guessing about what is permissible, leading to a cautious approach that impedes technological advancement.

Internationally, the U.S. increasingly finds itself at a competitive disadvantage. With more than 130 out of 194 countries having national data privacy laws, many foreign markets have clearer rules that facilitate stronger consumer trust. When competing abroad, U.S. companies often have to adjust their data practices to comply with foreign regulations, adding further operational complexity and cost. Additionally, there is a growing lack of trust in U.S. companies regarding privacy protections, making it harder for them to form partnerships and expand internationally. Countries with stringent data privacy laws, such as those in the European Union, may be reluctant to allow U.S. companies to operate within their jurisdictions due to perceived risks associated with weak privacy protections as evidenced by the much-challenged transatlantic data transfer agreement, Privacy Shield, or may subject companies to heavy regulatory scrutiny, adding to compliance and legal costs.

The absence of a Federal privacy law also exacerbates the existing "race to the bottom" dynamic in data collection practices. Companies, driven by competitive pressures, over-collect data, risking privacy violations and eroding consumer trust. This not only harms individuals but also damages the reputation of the U.S. technology sector globally.

In sum, a comprehensive Federal privacy law is essential to establish clear "rules of the road" for data practices, foster innovation, and maintain the U.S.'s leadership in the global technology arena. By promoting data minimization and responsible data use, such a law would enhance consumer trust and create a more predictable and stable environment for technological advancement.

Privacy for Responsible AI Innovation

We know from experience that when companies do not have bright lines to follow, businesses can compete in a race to the bottom—in this case to over-collection of data that violates our privacy.

Question 1. How would a bright line in a national privacy standard help companies innovate?

Answer. A bright line in a national privacy standard would substantially enhance companies' ability to innovate by providing clear, consistent guidelines on data collection and usage. Without a unified Federal privacy law, businesses face a fragmented regulatory landscape, where they must navigate varying state laws, leading to increased compliance costs and operational inefficiencies. This patchwork approach benefits larger incumbents that can afford these expenses, while smaller companies struggle to keep pace.

A national privacy standard would serve to eliminate the "race to the bottom" dynamics currently observed, where companies compete by over-collecting data to gain a competitive edge. Clear, bright-line rules would define acceptable data collection practices, thereby reducing the likelihood of privacy violations and the resultant legal battles, benefiting both consumers and smaller companies. This certainty is crucial for businesses focused on executing innovative strategies rather than being bogged down by legal uncertainties and potential lawsuits.

For AI companies, which rely heavily on vast amounts of data to train and fine-tune their models, a clear national standard would provide necessary legal clarity. Companies would know precisely what data practices are permissible, fostering an environment conducive to responsible innovation. This would minimize the risk of expensive court battles and regulatory scrutiny, allowing companies to invest more confidently in research and development.

Furthermore, a national privacy standard would bolster consumer trust. Informed consent and transparency about data use are critical components of such a standard. When consumers are assured that their data is handled responsibly and their privacy is protected, they are more likely to engage with new technologies. This increased engagement drives the adoption of innovative products and services, fueling further innovation.

In summary, a bright line in a national privacy standard would provide the regulatory clarity needed to streamline compliance, reduce legal risks, and foster an environment where innovation can thrive. It would help to level the playing field, allowing both large and small companies to focus on advancing technology while safeguarding consumer rights, thereby driving the next wave of technological progress.

Question 2. As AI continues to develop, how do you foresee the future of privacy if we do not provide bright lines about data collection and use—and responsible innovation?

Answer. As AI continues to develop, the future of privacy looks increasingly precarious without clear, stringent guidelines on data collection and use. Without these "bright lines," several concerning scenarios could unfold.

Firstly, the absence of clear regulations frequently leads to rampant over-collection of personal data. Companies driven by competitive pressures may try to collect as much data as possible to fuel their AI models. This practice not only violates privacy but also undermines consumer trust. The potential for data leaks and misuse increases exponentially as more data is collected, often without adequate safeguards, leading to untold and unnecessary consumer harms.

Moreover, the lack of explicit legal boundaries can result in prolonged legal battles as courts become the main battleground for defining acceptable data practices. This uncertainty can create a chilling effect on innovation, where businesses are hesitant to develop new technologies for fear of future legal repercussions. It could also take years for a relevant court case to ultimately make its way to the Supreme Court to resolve these issues definitively, leading to years of uncertainty and high legal costs for companies attempting to navigate the ambiguous regulatory landscape, with much of these costs eventually passed on to consumers.

Additionally, without clear guidelines, there is little to no incentive for companies, even those who desire to engage in better privacy practices, to invest in privacy-enhancing technologies (PETs). The development and adoption of PETs, such as differential privacy and federated learning, are critical for protecting user data while enabling innovative uses of AI. The lack of regulatory pressure to adopt these technologies can lead to invasive business practices and further consumer harm. Relying on the voluntary adoption of privacy preserving practices is an incomplete solution. Ultimately, privacy, security, and consumer data protection practices are most effective when paired with robust policies based on a comprehensive framework of protections.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BEN RAY LUJÁN TO UDBHAV TIWARI

Question 1. What does your research show on how AI companies' use of publicly available data to train and fine-tune their AI models is impacting the creative sectors—including but not limited to independent artists, authors, journalists and musicians?

Answer. While Mozilla has not conducted extensive research on the impact of AI's impact on the creative sector specifically, what we have observed in the AI field thus far indicates that the use of publicly available data by AI companies to train and fine-tune their models has significant impacts on creatives, including independent artists, authors, journalists, and musicians.

Firstly, many creatives have reported that their works are being used without consent to train AI models, leading to a loss of control over their intellectual property—often by ignoring existing mechanisms like the Robots Exclusion Protocol (through robots.txt files), which indicates to web crawlers which portions of web pages they are permitted to access and long served as a foundational tool of the modern web—but which is now proving insufficient to protect online data in the face of rampant collection practices by AI companies. This issue is exacerbated by the

lack of transparency in how these datasets are compiled, often without the knowledge or permission of the creators whose works are included. For example, the AI-generated art market has seen substantial growth, but this has led to widespread concerns about copyright infringement and the ethical use of artistic works, especially when end users can request art in the style of certain artists whose work was used to train AI models, often without the artists knowledge or consent.

Moreover, the economic implications for creatives are profound. As AI models become capable of generating high-quality content, indistinguishable in many cases from human-created works, there is a growing fear among creators of being displaced. Independent artists, authors, and musicians find themselves competing against AI-generated content, which can be produced at a fraction of the cost and time it takes a human creator. This competition can lead to reduced income opportunities and potentially undermine the value of human creativity.

Additionally, the rise of AI in journalism has led to concerns about the quality and integrity of news. Automated systems can generate articles and reports, but they often lack the nuanced understanding and investigative depth that human journalists provide.

In summary, while AI offers potential benefits in terms of efficiency and new forms of creativity, potentially unlocking access to artistic expression for those without the expertise to create music or art without AI tools, current practices regarding the use of publicly available data by the AI industry—including the legal uncertainty surrounding the question of rights holders' consent—pose significant challenges to the creative industries. Ethical considerations and robust policies are needed to protect the rights and livelihoods of independent creators and ensure that AI development progresses responsibly.

Question 2. What rights does Mozilla believe all individuals should have with respect to the use of their public data to train AI?

Answer. Mozilla firmly believes that individuals should have robust rights regarding the use of their public data to train AI models. These rights are fundamental to ensuring transparency, consent, and trust in the rapidly evolving AI landscape.

First and foremost, Mozilla advocates for the principle of informed consent. Individuals should be meaningfully informed about how their data will be used and should have the opportunity to provide explicit consent before their data is used to train AI models. This transparency empowers users to make knowledgeable decisions about their personal information. It is not enough to bury consent in lengthy terms and conditions; clear, concise, and easily understandable information to laypersons should be provided.

Secondly, Mozilla supports the right to opt-out. If consent is not initially obtained, individuals should have the ability to opt-out of having their data used for AI training at any time, through a process that is straightforward and user-friendly. This right ensures that individuals retain control over their personal data and can withdraw it from use if they choose.

Additionally, individuals should have the right to access and correct their data. This means that people can review what data has been collected about them, understand how it is being used, and request corrections to any inaccuracies. This transparency and accuracy are crucial for maintaining trust and ensuring that AI models are based on reliable data.

Moreover, Mozilla believes in the right to data minimization. Only the data necessary for specific, legitimate purposes should be collected and used. This principle reduces the risk of privacy breaches and limits the potential for misuse of personal information. It aligns with Mozilla's broader advocacy for privacy by design, ensuring that privacy considerations are integrated into AI development from the outset.

Question 3. What do you believe generative AI's impact will be on the data broker industry?

Answer. Generative AI's impact on the data broker industry is poised to be substantial, driving significant changes in data collection, utilization, and revenue streams. Initially, the rise of generative AI has created a surge in demand for large datasets. As AI companies rush to amass the vast amounts of data needed to train and fine-tune their models, data brokers find themselves in a lucrative position with access to data now in high demand.

However, this growth comes with severe long-term implications. The widespread use of generative AI for data collection raises concerns about privacy and the ethical use of personal information. Data brokers, traditionally operating with limited oversight, may face increased scrutiny as the public and regulators become more aware of how personal data is being utilized in AI development. The Protecting Americans' Data from Foreign Adversaries Act of 2024, which prohibits the sale of Americans' personal and sensitive data to foreign adversaries, and California's DELETE Act are

examples of steps towards addressing these concerns but highlights the need for broader regulation.

Question 4. On April 24th, President Biden signed into law the Protecting Americans' Data from Foreign Adversaries Act of 2024—which prohibits data brokers from selling, licensing or transferring Americans' personal and sensitive data to foreign adversaries.

a. Do you believe that this step puts adequate guardrails in place for data Brokers?

i. If not, what additional rights and protections do you believe Americans deserve with respect to the sale and transfer of their personal data by data brokers? Please refer to any specific legislation or parts of legislation that Mozilla believes are strong policy proposals.

Answer. The Protecting Americans' Data from Foreign Adversaries Act of 2024 is a significant step towards safeguarding American personal data from being accessed by foreign adversaries. While it addresses a critical national security concern, it does not comprehensively protect Americans' personal data in all contexts.

Firstly, the Act's focus on foreign adversaries leaves substantial gaps in data protection within the U.S. It does not address the broader issue of data brokers selling personal data to domestic entities or foreign entities not classified as adversaries or the potential for the use of intermediaries who would sell data on to those adversaries. This means that Americans' sensitive data can still be extensively traded and used within a complex web of transactions that ultimately undermines privacy. Data that is collected can be extremely sensitive, including unprotected health data and geolocation data which may lead to individual privacy and safety risks. Mozilla has previously *applauded previous Federal efforts to take on the Data Broker Ecosystem.* In addition, the act has a somewhat more narrow definition of what a data broker is than some existing state laws which more fully cover the spectrum of the data brokerage industry.

Mozilla believes additional protections, including the creation of public data broker registries, are necessary to fully safeguard Americans' personal data. One crucial step is the establishment of comprehensive Federal privacy legislation. Such legislation should encompass several key rights and protections including:

1. *Right to Informed Consent:* Individuals should have clear, comprehensible information about how their data is collected, used, and shared. Explicit consent should be obtained before any data transaction.
2. *Right to Opt-Out:* Individuals should be able to opt-out of data collection and sharing practices easily and at any time, without facing barriers or penalties.
3. *Right to Access and Correction:* Individuals should have the right to access the data collected about them and correct any inaccuracies, ensuring that their data is up-to-date and accurate.
4. *Data Minimization:* Only data necessary for specific, legitimate purposes should be collected and retained. This reduces the risk of misuse and enhances overall data security.
5. *Transparency and Accountability:* Companies should be required to provide transparency reports detailing their data practices and be held accountable for violations of privacy standards.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. RAPHAEL WARNOCK TO UDBHAV TIWARI

Civil Rights and Antidiscrimination

In your written testimony, you describe how AI can "infer sensitive attributes about individuals, leading to potential privacy violations if used for targeted content or discrimination." Some Federal agencies have already taken action against online platforms for violating Federal anti discrimination laws.

Question 1. In what ways do existing Federal antidiscrimination laws fail to adequately protect consumers against online discrimination?

Answer. Existing Federal anti-discrimination laws, while foundational, fail to adequately protect consumers against the unique challenges posed by online discrimination, particularly when it comes to the use of artificial intelligence (AI) and automated systems.

Firstly, traditional anti-discrimination laws like the Civil Rights Act of 1964 and the Fair Housing Act were crafted long before the advent of AI and digital platforms. These laws do not explicitly address the complexities of algorithmic bias and

discrimination that can occur in online environments. AI systems, when trained on biased datasets, can inadvertently perpetuate and even amplify existing societal biases in ways that are extremely difficult to detect or for auditors to demonstrate disparate impact resulting from these algorithms. This can lead to discriminatory outcomes in various domains such as employment, lending, and housing, where automated decision-making tools are increasingly used.

Furthermore, enforcement of existing laws by Federal agencies such as the Federal Trade Commission (FTC) and the Department of Justice (DOJ) has been challenging due to the opaque nature of AI algorithms. These agencies often lack the necessary resources and technical expertise to effectively scrutinize and regulate AI-driven discrimination.

Although the FTC has issued guidelines and warnings about AI fraud and discrimination, these measures are not sufficient given the rapid pace of AI development and deployment.

The limitations of current laws are exacerbated by the lack of transparency in how AI systems make decisions. Without clear guidelines on algorithmic accountability and transparency, it is difficult to identify and rectify instances of discrimination. Consumers often have no way to understand how decisions affecting them are made or to contest these decisions. This can prove critical when AI systems increasingly control important aspects of individual's lives including access to housing, financial resources, and even their livelihoods through gig platforms.

Moreover, existing laws do not further enable more proactive measures such as bias audits or impact assessments for AI systems. Such provisions are crucial for identifying and mitigating discriminatory practices before they cause harm. Lessons can be drawn from state-level regulations and international frameworks that have started to incorporate requirements for bias audits and impact assessments.

Question 2. In your view, are Federal agencies adequately enforcing existing anti-discrimination laws against companies using AI tools? Are there additional steps that Federal agencies should take to enforce existing laws?

Answer. Federal agencies such as the Federal Trade Commission (FTC), the Equal Employment Opportunity Commission (EEOC), and the Department of Justice (DOJ) have made notable efforts to enforce existing anti-discrimination laws against companies using AI tools including through the *EEOC's AI technical assistance document,* but these efforts are not yet adequate given the rapid and complex developments in AI technology.

The FTC has issued guidelines and warnings concerning AI fraud and discriminatory practices, emphasizing the need for fairness and transparency in AI applications. However, the agency's current resources and technical expertise are often insufficient to keep pace with the sophisticated and opaque nature of AI algorithms and exponential growth of the use of AI across myriad applications. The FTC's ability to conduct in-depth investigations and enforce compliance is limited by these constraints, which hinders its effectiveness in addressing AI-driven discrimination comprehensively.

Similarly, the DOJ has taken steps to address discrimination through various initiatives and enforcement actions. However, the DOJ's approach to AI-related discrimination is broadly reactive rather than proactive. The current legal framework does not mandate regular audits or assessments of AI systems for bias, leaving significant gaps in preventive measures.

Mozilla has studied the potential for *Accelerating Progress Towards Trustworthy AI* and released a report on the subject in early 2024. In addition to the insights detailed in the report, we recommend that to enhance the enforcement of existing laws, Federal agencies should consider the following additional steps:

1. *Increase Technical Expertise and Resources:* Agencies need to invest in technical expertise to better understand and scrutinize AI algorithms. This includes hiring data scientists and AI specialists who can identify and mitigate bias in AI systems.
2. *Bias Audits and Impact Assessments:* Legislation should push companies in high-risk sectors to conduct regular bias audits and impact assessments of their AI tools. These audits should be transparent and results should be publicly accessible to ensure accountability.
3. *Enhance Transparency Requirements:* Certain companies in high-risk sectors using AI should be required to disclose how their algorithms make decisions, including the data sources and methodologies used. This transparency will enable both consumers and regulators to identify potential biases and discriminatory practices.

4. *Collaboration with State and International Bodies:* Learning from existing state-level regulations and international frameworks, such as the GDPR in Europe, can provide valuable insights into effective AI governance and enforcement practices, as well as what to avoid.

Question 3. In establishing new anti discrimination provisions in a Federal data privacy law, what specific provisions should Congress consider, and what are the key lessons from state-level and international regulations on similar topics?

Answer. Federal agencies such as the Federal Trade Commission (FTC) and the Department of Justice (DOJ) have made notable efforts to enforce existing anti discrimination laws against companies using AI tools, but these efforts are not yet adequate given the rapid and complex developments in AI technology.

The FTC has issued guidelines and warnings concerning AI fraud and discriminatory practices, emphasizing the need for fairness and transparency in AI applications. However, the agency's current resources and technical expertise are often insufficient to keep pace with the sophisticated and opaque nature of AI algorithms. The FTC's ability to conduct in-depth investigations and enforce compliance is limited by these constraints, which hinders its effectiveness in addressing AI-driven discrimination comprehensively.

To enhance the enforcement of existing laws, Federal agencies should consider the following additional steps:

1. *Increase Technical Expertise and Resources:* Agencies need to invest in technical expertise to better understand and scrutinize AI algorithms. This includes hiring data scientists and AI specialists who can conduct in-depth technical analyses into AI systems and corporate claims regarding AI.
2. *Enabling Bias Audits and Impact Assessments:* As discussed in depth in *Mozilla's comments on AI accountability to NTIA,* legislation should better enable the audits of companies in sensitive industries and which develop products critical to individuals' welfare, such as financial and healthcare tools, allowing for the conducting of regular bias audits and impact assessments of their AI tools. These audits should be transparent and results should be publicly accessible to ensure accountability.
3. *Enhance Transparency Requirements:* Certain companies in high-risk sectors using AI should be required to disclose how their algorithms make decisions, including the data sources and methodologies used. This transparency will enable consumers and regulators to identify potential biases and discriminatory practices.
4. *Collaboration with State and International Bodies:* Learning from state-level regulations and international frameworks, such as the GDPR in Europe, can provide valuable insights into effective AI governance and enforcement practices. Closely monitoring the implementation and efficacy of the EU's recently enacted AI Act, which puts forward several measures aiming to curb algorithmic discrimination and to protect the fundamental rights of people residing in the EU, is likely to prove worthwhile for regulators.

Targeting and Election Misinformation

In your written testimony, you discuss how generative AI "has led to advertisers created highly customized campaigns" to influence "unsuspecting" consumers. Similar technologies can also be applied to influence unsuspecting voters, and we have already seen examples of how foreign actors have used generative AI to influence American policymaking.

Question 4. In crafting data privacy legislation, how can Congress help ensure that consumers' data is not unknowingly used against them in crafting influence campaigns, whether to influence purchase or voting behavior?

Answer. Congress can take several key steps to ensure that consumers' data is not unknowingly used against them in the crafting of influence campaigns, whether for purchasing behavior or voting decisions.

Firstly, establishing comprehensive Federal privacy legislation is essential. Such legislation should mandate clear and explicit consent requirements for data collection and use and consumers must be fully informed about how their data will be used. This transparency will empower individuals to make informed decisions about their data. For instance, provisions similar to the General Data Protection Regulation (GDPR) in the European Union could be adopted, which include stringent consent requirements and give individuals the right to know how their data is being processed.

Secondly, data minimization principles should be a cornerstone of any Federal privacy legislation. By limiting the amount of data collected to what is strictly nec-

essary for the specified purpose, the risks of data misuse in influence campaigns can be significantly reduced. This approach not only protects consumer privacy but also aligns with responsible data stewardship practices *advocated by Mozilla.*

Thirdly, implementing robust transparency and accountability mechanisms is crucial. Companies should be required to disclose how consumer data is collected, processed, and utilized, particularly in relation to influence campaigns. This includes revealing the sources of data used for targeted advertisements and influence operations. Enhanced transparency will enable consumers to better understand and control their data, reducing the likelihood of it being used against them without their knowledge.

Moreover, strong enforcement and oversight mechanisms must be established. Regulatory bodies should be empowered to audit and review companies' data practices, ensuring compliance with privacy laws. Penalties for violations should be significant enough to deter misuse of consumer data. The Federal Trade Commission (FTC) and other relevant agencies should be given the resources and authority needed to effectively monitor and enforce these regulations.

Additionally, promoting the development and adoption of privacy-enhancing technologies (PETs) can play a critical role in safeguarding users. Technologies such as differential privacy, which allows data to be used for analysis without compromising individual privacy, can help protect consumers from undue influence. By incentivizing the use of PETs, Congress can help ensure that consumer data is handled in a manner that respects privacy and reduces the risk of exploitation.

Finally, requiring clear labeling and disclosure of data sources and AI in political advertisements and marketing campaigns can further safeguard against misuse. Consumers have the right to know how their data has been used to target them and the origins of the information influencing their decisions.

Question 5. What requirements or best practices should Congress put in place to prevent foreign entities or other bad actors from using technology tools and platforms, including but not limited to generative AI, to create and spread election misinformation?

Answer. Former Mozilla senior fellow Renée DiResta, who during her *fellowship focused on media, misinformation, and trust,* has discussed how generative AI "takes the cost of creation to zero," which allows practically anyone to create compelling content.[1] However, actors seeking to spread misinformation still depend on platforms to distribute AI generated content. To prevent foreign entities or other bad actors from using technology tools and platforms, including generative AI, to create and spread election misinformation, Congress should implement a series of stringent requirements and best practices.

1. *Comprehensive Federal Privacy Legislation:* Establish robust privacy laws that restrict the collection, storage, and misuse of personal data. Such legislation should include strict consent requirements and data minimization principles to ensure that only necessary data is collected and used responsibly. These measures would reduce the amount of data available for misuse in disinformation campaigns by foreign entities.
2. *Enhanced Transparency Requirements:* Mandate that social media platforms and AI developers disclose the origins of content, particularly political advertisements and information related to elections. This should include clear labeling of content generated, influenced, or paid for by foreign entities. Platforms should provide transparency reports detailing the measures taken to prevent the spread of misinformation.
3. *Researcher Access for Platforms:* Require technology platforms to provide access to relevant internal data sources. This will help not only create transparency, but also create accountability and allow for a scientific understanding related to potential harms caused or enabled by platforms. This should include the mandatory sharing of critical platform data with researchers and academics (with adequate privacy protections) to allow for the independent scrutiny of platform practices. Proposals like the Platform Accountability and Transparency Act (PATA) would enable such transparency and a better understanding of what's occurring on platforms. It is for this reason that *Mozilla has led the call for Meta to continue supporting CrowdTangle,* at least through 2024, to ensure access to critical data for academics, journalists, and watchdogs.

---

[1] Interview—Online manipulation expert Renée DiResta: 'Conspiracy theories shape our politics in extremely mainstream ways", Alex Hern. The Guardian. 14 July 2024. Available here: *https://www.theguardian.com/technology/article/2024/jul/14/renee-diresta-invisble-rulers-internet-algorithms-media-disinformation-ai*

4. *Development and Use of AI for Detection:* Encourage and support the development of AI tools specifically designed to detect and mitigate the spread of misinformation. These tools can analyze content patterns, flag suspicious activities, and identify deepfakes and other forms of AI-generated misinformation.
5. *Funding and Support for Research:* Provide funding for research into the methods used by foreign entities to spread misinformation. This research can inform the development of new technologies and strategies to combat these efforts.
6. *Public Awareness Campaigns:* Launch educational initiatives to inform the public about the dangers of misinformation and how to identify it. Increasing public awareness can reduce the effectiveness of misinformation campaigns by promoting critical thinking and media literacy.
7. *Legislative Measures Similar to the Protecting Americans' Data from Foreign Adversaries Act:* Enact additional legislation targeting the specific practices used by foreign entities to spread misinformation. This includes measures to prevent the sale and transfer of personal data to foreign adversaries and to enhance cybersecurity protocols.

Public Understanding of AI and Transparency

Pew Research recently reported that "only three-in-ten U.S. adults can correctly identify all six uses of AI asked about in the survey" and "44 percent think they do not regularly interact with AI." These numbers underscore the limited public understanding of how often AI is currently used, much less how consumer data may be used to train AI models.

Question 6. In crafting consumer consent and notice provisions, how should Congress best ensure that any information provided to consumers is comprehensible given the current limited understanding of AI and data privacy policies?

Answer. In crafting consumer consent and notice provisions, Congress must ensure that the information provided to consumers is both comprehensible and accessible, addressing the current limited and evolving understanding of AI and data privacy policies via Federal privacy legislation. To achieve this, several key strategies should be implemented:

1. *Plain Language Requirement:* Legal and technical jargon often renders privacy policies incomprehensible to the average consumer. Congress should mandate that all consumer notices and consent forms be written in plain, straightforward language. This approach ensures that consumers can easily understand the terms of data use without requiring specialized knowledge.
2. *Standardized Formats:* To facilitate better understanding and comparison, Congress should standardize the format of privacy notices. This could include the use of clear headings, bullet points, and summaries that highlight the most critical information upfront as well as standardizing the timing of when privacy notices are shown to users—ideally right before they start to use a tool or website. In addition, creating a standardized navigation format with a functional table of contents to enable users to easily find specific information is critical to ensuring better understanding among users. A standardized format can help consumers quickly grasp the essentials of what they are consenting to.
3. *Layered Notices:* Implementing layered notices can improve comprehension by presenting information in manageable chunks. The initial layer should provide the most important information concisely, with additional layers offering more detailed explanations. This approach allows consumers to obtain a quick overview while retaining the option to delve deeper into the specifics as needed.
4. *Visual Aids and Interactive Elements:* Incorporating visual aids such as icons, infographics, and interactive elements can help convey complex information more effectively. These tools can simplify the presentation of data practices and consent options, making it easier for consumers, including those with low literacy skills, to understand and make informed decisions.
5. *Accessibility Standards:* Notices and consent forms must be accessible to all individuals, including those with disabilities. This includes ensuring compatibility with screen readers, providing text alternatives for visual content, and using accessible fonts and color contrasts.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TED CRUZ TO
UDBHAV TIWARI

Take It Down Act

In my opening statement, I referenced how artificial intelligence (AI) can be used for nefarious purposes and how Congress should pursue targeted, tailored solutions that address specific harms or issues. It's why Sen. Klobuchar and I introduced the Take It Down Act, which targets bad actors who use AI to create and publish fake, lifelike images of real people—oftentimes teenage girls—in sexually explicit situations. It also gives recourse for victims to get the images taken down.

Question 1. Do you support the policy in the Take It Down Act and agree that Congress should act to stop the proliferation of revenge porn, including deep fake pornographic images of adults and children?

Answer. We're extremely supportive of the goals of the legislation and making sure that vulnerable people, especially minors, aren't harmed by non-consensual intimate imagery (NCII) and have ways to fight back. We commend Sens. Cruz and Klobuchar's leadership on this issue and agree that Congress should act to help mitigate the terrible harms caused by NCII. In addition, we believe that Congress and tech companies can have further impact by investing in research and development of open-source tools to identify and combat AI generated content, like non-consensual deep fakes.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELLEY MOORE CAPITO TO
UDBHAV TIWARI

Question 1. In your testimony you covered the importance of investing in privacy-enhancing technologies and how they help reduce risk while also allowing for innovation. How can Congress ensure that small businesses have equal access to these technologies?

Answer. In our testimony, Mozilla emphasized the critical role that privacy-enhancing technologies (PETs) play in reducing risks and fostering innovation. To ensure that small businesses have equal access to these technologies, Congress can take several strategic steps:

1. *Public Research Funding and Grants:* Congress should allocate public research funding specifically for the development and deployment of PETs. This funding should come with stipulations that the research outputs are made publicly available, thereby ensuring that small businesses can benefit from cutting-edge advancements without incurring prohibitive costs. Grants and subsidies targeted at small and medium-sized enterprises (SMEs) can further support their adoption of PETs.
2. *Support for Open-Source Projects:* Encouraging and funding open-source projects can significantly enhance the accessibility of PETs. Open-source software proliferates quickly among small businesses due to minimal costs and the absence of vendor lock-in. By supporting initiatives that develop open-source PETs, Congress can help democratize access to these essential tools. In 2024, Mozilla *brought together over 40 leading scholars and practitioners* working on openness and AI; while focused on artificial intelligence rather than PETs, the event participants repeatedly emphasized the benefits of open-source for making it easier to identify potential privacy harms, highlighting the myriad benefits of openness.
3. *Public-Private Partnerships:* Establishing partnerships between government agencies, academic institutions, and private sector companies can foster the development and dissemination of PETs. These collaborations can provide small businesses with access to resources, expertise, and technologies that might otherwise be out of reach.
4. *Tax Incentives and Credits:* Offering tax incentives or credits to small businesses that invest in PETs can lower the financial barriers to adoption. These incentives can encourage SMEs to prioritize privacy and security in their operations without sacrificing their limited budgets.
5. *Technical Assistance and Training Programs:* Providing technical assistance and training programs can help small businesses understand and implement PETs effectively. Congress can support initiatives that offer workshops, online courses, and consulting services to educate SMEs about the benefits and applications of privacy-enhancing technologies.

6. *Development of Public AI Infrastructure:* Congress can support the creation of publicly accessible AI infrastructure, such as cloud-based platforms, that incorporate PETs. This infrastructure can be made available to small businesses at reduced costs, providing them with the tools they need to innovate while maintaining privacy standards.
7. *Incentivizing Industry Standards:* Encouraging the development and adoption of industry standards for PETs can level the playing field. Standards ensure that all businesses, regardless of size, can integrate privacy-enhancing technologies into their operations in a consistent and interoperable manner.

Question 2. You discussed in your testimony the need to update existing protections in order to protect sensitive data from kids and sensitive categories like health data. We see these camera filters and other social media tools that are meant to engage our youth, but I worry about the data that is then being collected on our young people when they engage in these features, like their images and likenesses. Recently, Brazil has blocked Meta from using social media posts and data from minors to train its AI models. How can Congress work with industry to protect our young people so that they can engage with these features while protecting their images and likenesses?

Answer. Beyond passing a Federal privacy law with clear rules of the road for the collection, storage, and use of children's data, Congress could work directly with industry as well as relevant civil society organizations to establish voluntary commitments. By using its convening power, Congress could create an environment where the largest relevant platforms would be able to work together, with Congressional oversight, to create guardrails and industry standards. While not legally binding, by working to create voluntary standards Congress could help to mitigate some of the current harms and "race to the bottom" dynamics that affect children's privacy today.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED CRUZ TO MORGAN REED

Take It Down Act

In my opening statement, I referenced how artificial intelligence (AI) can be used for nefarious purposes and how Congress should pursue targeted, tailored solutions that address specific harms or issues. It's why Sen. Klobuchar and I introduced the Take It Down Act, which targets bad actors who use AI to create and publish fake, lifelike images of real people—oftentimes teenage girls—in sexually explicit situations. It also gives recourse for victims to get the images taken down.

Question 1. Do you support the policy in the Take It Down Act and agree that Congress should act to stop the proliferation of revenge porn, including deepfake pornographic images of adults and children?

Answer. We appreciate your work on this important issue. From our perspective, when it comes to AI, Congress should focus first and foremost on observed harms and should be skeptical of calls to legislate in areas where harms are speculative and theoretical. So, we think it's entirely appropriate for you to legislate and clarify liability for publishing deepfake revenge porn. I think it's important that any legislation in this space strike a balance that deters and punishes bad actors, while safeguarding foundational protections in online marketplaces. Part of that is distinguishing adequately between social media platforms with public facing audiences and secure messaging services that should be empowered to protect individuals' privacy. But we hope to work with you on the right formula for legislation on this issue.

Consequences of Adopting EU Regulatory Model

During the hearing there was much discussion over how new regulatory burdens in the American Privacy Rights Act would even exceed European Union (EU) requirements and put small and medium-sized businesses at a comparative disadvantage against giant corporations. During my opening statement, I cautioned against the United States adopting an EU style regulatory system on data privacy and AI.

Question 1. What does the United States lose if we go the direction of Europe and adopt heavy government intervention and control over our technology and entrepreneurs, particularly with respect to small businesses?

Answer. Adopting the European Union's burdensome regulatory approach would significantly hurt U.S. small businesses, innovation, and technological competitiveness. The EU's regulatory approach generally imposes stringent *ex ante* requirements that limit businesses' ability to innovate and adapt to technological advance-

ments. Adopting a philosophy of regulating first and asking questions later would disproportionately affect small businesses, many of which do not have the same resources as their larger counterparts to contend with legal or compliance challenges.

While larger firms have compliance *departments,* smaller firms often lack the resources to hire employees dedicated solely to compliance. With a comparative advantage in compliance, *ex ante* regulation of emerging technologies tends to inure to the benefit of big companies, while small businesses' comparative advantage in adaptation and innovation is nullified. Accordingly, *ex ante* regulation of emerging technologies, especially prior to any level of market adoption or maturity, would effectively solidify and expand large businesses' existing market advantages in adjacent industries while subjecting small businesses to financial and logistical constraints that hinder their competitiveness.

Although many App Association members have spent significant precious resources coming into compliance with the EU's General Data Protection Regulation (GDPR), it provides an interesting case study in how burdensome regulations affect innovative small business investment and growth. According to a 2018 study published by the U.S. National Bureau of Economic Research, venture capital invested in EU technology businesses decreased by more than 50 percent shortly after the GDPR came into effect.[1] Venture capital is crucial for funding early-stage companies, which may struggle to scale or innovate without it. Replicating similar laws in the United States would dissuade venture capitalists from investing in small and medium-sized businesses and take away a key source of funding from some of the country's most innovative companies. I know that some policymakers are considering stepping into the AI services markets before they have even formed yet, and I think this is a bad idea. In particular, the Federal Trade Commission (FTC) and the United Kingdom's Competition and Markets Authority (CMA) are aggressively investigating and casting a shadow on significant investments by cloud companies into AI firms. The problem with these threats is that AI firms need large sums to train models, and they need cloud companies to make those investments because those are the savvy investors with the complementary resources to help AI services market entrants actually succeed and credibly compete with the giants. There is a serious risk that government agencies will kill emerging markets in the cradle because they do not like the firms making the investments.

Finally, overly broad regulation could hurt U.S. global competitiveness in technology. Artificially slowing innovation through premature government intervention, such as the EU's GDPR and Digital Markets Act (DMA), will leave room for other parties, including bad actors, to create critical technologies and capture greater global market shares. While policymakers should enact regulations that protect businesses and consumers, such as a preemptive Federal privacy law, following the example set by the European Union, would decelerate innovation and enable foreign companies to overtake U.S. companies.

Question 2. During the hearing, you spoke favorably over the positive uses that AI innovation can bring to the quality of life for Americans and for growing small business jobs. How would adopting an EU regulatory model in the United States put AI innovation at risk?

Answer. Pursuing a similar regulatory model as the EU would slow AI innovation in the United States and place the AI-powered tools that U.S. consumers and small businesses use daily at risk. From Smart Yields' smart AgTech that helps farmers increase crop yield to Canned Spinach's AI-powered software development, U.S. businesses have produced AI systems that have been quickly integrated into a number of industries and provide significant benefits to both consumers and business owners alike.[2] Under heavy regulatory burdens like those present in the EU, these AI advancements could be delayed or fail to reach their full potential. For example, if the United States were to enact legislation with overly strict data minimization prohibitions—especially if those provisions generally prohibit processing of data, with limited exceptions—Congress might inadvertently eliminate AI developers' access to the large datasets essential to training and improving models and prevent the introduction of innovative AI solutions into the market.

Moreover, in order to meet the requirements of an EU-style regulatory model, small businesses would have to devote significant funding to legal and compliance measures. This would effectively limit their resources to build new AI products or hire personnel, decreasing both the number of AI-powered tools on the market and

---

[1] Jia, Jian, *et al.,* 2018, *The Short-Run Effects of GDPR on Technology Venture Investment, https://www.nber.org/papers/w25248.*

[2] "Home: Smart Yields: Realtime Analytics & AI-Powered AgTech." *Smart Yields* | Together We Can Farm SmarterSM, 10 Apr. 2024, smartyields.tech/#technology. "Home." *Canned Spinach,* 17 Jan. 2024, cannedspinach.com/.

small business job growth. In turn, the regulation would effectively hinder technological growth and U.S. global competitiveness in the industry.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. SHELLEY MOORE CAPITO TO MORGAN REED

Question 1. In your written testimony, you discussed the potential for AI to improve Americans' lives through cloud computing. Along with being expensive, AI computing power requires a massive amount of energy. For example, one query on ChatGPT takes 18 times the energy of a Google search. Does our energy grid have the capacity to handle AI at the rate that these systems are excelling? What does Congress need to do to ensure that our grid is equipped to handle the extra burden that AI computing puts on it?

Answer. The rapid advancement of AI has posed challenges to our current energy infrastructure due to its significant power requirements. As you noted, AI tools can consume more power than traditional digital activities, which can strain existing energy infrastructure. To ensure that our grid can accommodate growing demand from AI, policymakers should take three steps. First, policymakers should invest in modernizing infrastructure, including upgrading transmission lines, enhancing storage capabilities, and integrating smart grid technologies that enable providers to dynamically manage energy loads and optimize efficiency. Second, policymakers should promote the addition of renewable energy sources that can help meet increased energy demands of AI without exacerbating environmental impacts. Finally, policymakers should partner with private enterprises and support research and development initiatives designed to accelerate the advancement of more energy-efficient computing technologies, on-device processing, and AI systems that require less power than current models. Many AI businesses have released AI systems with lighter weights that require less energy than popular models. For example, OpenAI recently released GPT–4o mini, a small language model that requires less computational power and energy resources to run than the company's other recent models, yet still performs at similar standards.[3]

Additionally, while AI increases energy consumption, it can also offer solutions to enhance energy efficiency across various industries, reduce greenhouse gas emissions, help electricity providers optimize operations, create jobs in the energy market, and more.[4] For example, the energy sector can use AI to monitor power flows, predict consumer demand, and maintain reliable grid operations.[5]

Question 2. The Artificial Intelligence (AI) Research, Innovation, and Accountability Act that I am a lead cosponsor of would establish a framework for greater transparency, accountability, and security for high-impact AI systems. This bill would require NIST to research standards and applications for showing authenticity and ownership of content published online. How important is it for people publishing content online to have assurances that their work will carry a mark of their ownership, and is that enough of a deterrent for bad actors? What do you believe will happen if AI continues to progress and is left unchecked by the Federal government?

Answer. We appreciate your focus on appropriate regulations for AI systems. Enacting regulation that supports its progress will ensure that U.S. consumers can continue to take advantage of useful AI tools, support job creation and economic growth, and boost U.S. global technological competitiveness. However, we have concerns that premature or broad legislation that requires additional oversight by Federal agencies may impede the development of AI tools and make it more difficult for U.S. businesses to innovate. Moreover, legislation that increases regulatory burdens will have a disproportionate impact on small businesses, which do not have the same resources as their larger counterparts to come into compliance. We wel-

---

[3] Sophia, Deborah. "OpenAI Unveils Cheaper Small AI Model GPT–4o Mini." *Reuters,* 18 July 2024, *https://www.reuters.com/technology/artificial-intelligence/openai-unveils-cheaper-small-ai-model-gpt-4o-mini-2024-07-18/*. Accessed 8 Aug. 2024.

[4] "It's Not Easy Being Green . . . Or Is It?" *ACT | The App Association,* 21 Nov. 2022, *https://actonline.org/2022/11/21/its-not-easy-being-green-or-is-it/*. Accessed 8 Aug. 2024.

[5] Rozite, Vida, *et al.,* "Why AI and Energy Are the New Power Couple." *International Energy Agency,* 2 Nov. 2023, *https://www.iea.org/commentaries/why-ai-and-energy-are-the-new-power-couple.* Accessed 8 Aug. 2024.

come the opportunity to work with you on developing legislation that achieves the same goals of protecting U.S. consumers while bolstering innovation.

○