S. HRG. 119–205

PROTECTING THE VIRTUAL YOU: SAFEGUARDING AMERICANS' ONLINE DATA

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JULY 30, 2025

Serial No. J–119–35

Printed for the use of the Committee on the Judiciary

www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
61–893 WASHINGTON : 2026

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

LINDSEY O. GRAHAM, South Carolina	RICHARD J. DURBIN, Illinois, *Ranking Member*
JOHN CORNYN, Texas	SHELDON WHITEHOUSE, Rhode Island
MICHAEL S. LEE, Utah	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	CHRISTOPHER A. COONS, Delaware
JOSH HAWLEY, Missouri	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	MAZIE K. HIRONO, Hawaii
JOHN KENNEDY, Louisiana	CORY A. BOOKER, New Jersey
MARSHA BLACKBURN, Tennessee	ALEX PADILLA, California
ERIC SCHMITT, Missouri	PETER WELCH, Vermont
KATIE BOYD BRITT, Alabama	ADAM B. SCHIFF, California
ASHLEY MOODY, Florida	

KOLAN DAVIS, *Chief Counsel and Staff Director*
JOE ZOGBY, *Democratic Chief Counsel and Staff Director*

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

MARSHA BLACKBURN, Tennessee, *Chair*

LINDSEY O. GRAHAM, South Carolina	AMY KLOBUCHAR, Minnesota, *Ranking Member*
JOHN CORNYN, Texas	CHRISTOPHER A. COONS, Delaware
JOSH HAWLEY, Missouri	RICHARD BLUMENTHAL, Connecticut
JOHN KENNEDY, Louisiana	ALEX PADILLA, California
ASHLEY MOODY, Florida	ADAM B. SCHIFF, California

BEN BLACKMON, *Republican Chief Counsel*
DAN GOLDBERG, *Democratic Chief Counsel*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

PROTECTING THE VIRTUAL YOU: SAFEGUARDING AMERICANS' ONLINE DATA

WEDNESDAY, JULY 30, 2025

UNITED STATES SENATE,
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY,
AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice at 2:47 p.m., in Room 226, Dirksen Senate Office Building, Hon. Marsha Blackburn, Chair of the Subcommittee, presiding.

Present: Senators Blackburn [presiding], Klobuchar, and Schiff.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A U.S. SENATOR FROM THE STATE OF TENNESSEE

Chair BLACKBURN. The Subcommittee on Privacy, Technology, and the Law will come to order. And Senator Klobuchar is on her way. She'll be here in a couple of minutes, but we will go ahead and begin since we do have five witnesses. And we thank each of you for giving your time and being here today.

Today, we are going to put our attention on what I think is one of the most consequential issues up for discussion when we talk about the virtual space, and that is how does each and every individual American preserve their privacy and their personal data in the virtual space? The title of the hearing, Protecting the Virtual You: Safeguarding American's Online Data.

This speaks to what is becoming a growing connection between you, and the physical space, and what you are doing each and every day in your transactional life, in the virtual space, or the digital version of your yourself. And this comes through how companies collect, track, and monetize your data. And every single bit of that is done without your consent or your knowledge.

In today's economy, data is currency. Everything from your shopping habits to your health information, your children's online activity, to your political views can be identified, sold, and resold, often with little transparency or recourse. Meanwhile, consumers are left to decipher lengthy privacy policies and click "agree" at the bottom of the page even before they can begin to access any online service.

The absence of a comprehensive national data privacy framework has left millions of Americans vulnerable. While numerous States have enacted privacy laws, the result has been a patchwork that fails to provide the clarity, consistency, and confidence that consumers and responsible businesses need and deserve. For years now, I have been clear we need a national privacy standard that

is comprehensive and enforceable, one that empowers consumers, promotes innovation, and ensures accountability. It should prioritize transparency, minimize data collection, and provide meaningful consent, not just a box to check.

We have a panel of witnesses here this afternoon who all agree that there is an urgent need for a comprehensive bill. Now, there's probably going to be some disagreement about how we get to that national standard, but we can agree on one thing; it is past time for Congress to take up this issue, to take action to pass a bill and see that bill signed into law.

We should also acknowledge how closely this issue is tied to the safety of our children online. Senator Blumenthal and I have worked diligently on the Kids Online Safety Act, which would require platforms to design their product for children's well-being in mind, not just for their bottom line. We've seen time and again how data-driven algorithms target kids with addictive content and expose them to harmful material. Business models that profit from children's vulnerabilities must be reined in.

It is absolutely disgusting that our children are the product when they are online. And through the Open App Market Act that I introduced with Senator Klobuchar, I have worked to increase competition and consumer choice in the digital marketplace. Whether it's protecting your personal data, your right to download the apps you want, or your ability to access services, the common thread is this; users not tech giants should be in control of the individual users' life.

Today's hearing will explore core principles that should go into a national data privacy framework that reflect American values. We'll ask what categories of personal data deserve background protection? How can we give consumers real control over how their data is used, and how do we ensure that AI systems which are only growing more powerful or accessing and using consumer's data and information in a responsible way?

As artificial intelligence becomes increasingly embedded in everyday life from how we shop to how we work, communicate, and make decisions, Americans deserve to know when, where, and how their data's being used to shape their online experiences. We have an opportunity and a responsibility to get this right, and I am looking forward to your testimony today, and to the questions that we will have as we move forward.

Senator Klobuchar, you're recognized.

OPENING STATEMENT OF HON. AMY KLOBUCHAR, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Senator KLOBUCHAR. Well, thank you very, Chair Blackburn, and thank you to all of our witnesses. And I'm really grateful for your leadership on these issues, Madam Chair, and your willingness to work with me, and Senator Blumenthal, and many others.

We all know new technologies have made it easier for people to monitor their health, collaborate with colleagues, communicate with loved ones, and more, but Federal law doesn't do enough, as we all know, to address the privacy that come with these innovations, the privacy concerns. Technology companies collect an enormous amount of personal information about our daily lives. They

know what we buy, who our friends are, where we live, where we work and travel, even how much we would be willing to pay for something.

Yet, for too long the Big Tech companies, many of which dominate the market that they operate in, have been telling American consumers, "Just trust us," even though their business models are designed to collect personal information and to use it for profit. The bottom line is that we are the product, we are and that's how many tech companies make their money, and a lot of it.

In 2024, Google and Meta earned a combined $420 billion in advertising revenues alone, and they made a lot more money because Americans lack privacy protections. And American's data earned Meta $68 in a single quarter last year. Think about that. All these people who don't realize that they're being tracked. But a European Facebook user with a comprehensive privacy protection only generated $23. And that money can be used for a lot of other things that people need right now.

And it seems like every day we hear a new story about companies playing fast and loose with data and taking advantage of customers. Earlier this year, a whistleblower from Facebook, now Meta, testified to another Subcommittee about how the company would track users so closely that it could identify when teenage girls felt emotionally vulnerable and then target them with ads exploiting these emotions. For example, when a teenage girl would delete a selfie, Facebook might serve her an ad for diet products.

Criminals also view huge troves of data as attractive targets for hacking. We've seen major data breaches ranging from the 2017 Equifax data breach that exposed sensitive financial information from more than 140 million individuals, to the hack of Change Healthcare affecting 190 million people and causing more than 100 electronic systems vital to the U.S. healthcare system to be shut down.

On my way here, I was on the phone with the mayor of St. Paul, Minnesota, because they, like so many other jurisdictions, are responding to a targeted cyberattack on their IT infrastructure, which has shut down some of the city's digital services and may have compromised city employee data.

Once in the hands of criminals, data can be used for everything from identity theft to more serious crimes and we all learned too tragically with the horrific murders in my State of my good friend Melissa Hortman, the former speaker of the House and her husband, Mark, how accessible personal data is including people's addresses because the murderer only killed the people and went to the houses, the people whose addresses he had.

Businesses are also using personal data collected across the internet in novel ways such as to set individualized prices designed to increase costs for consumers. Should a person—and this is a question we have to ask as Senators really have to submit to this kind of intrusive data collection just to send a message to a friend online, or to book a flight, or to order some diapers. I don't think so.

That's why more than 20 States have stepped in. I suspect today we'll hear from some of our witnesses about the patchwork of State laws. I agree it's a problem, but I believe we should have passed

privacy legislation many, many years ago. I advocated for it back then. We tried, and in fact, in 2019, I introduced a comprehensive privacy bill. I was a co-sponsor of Senator Cantwell, and Kathy, McMorris Rogers, a former Republican House Member.

The bill would've required companies to collect only the information necessary to provide the goods and services that consumers sought. Insured consumers consented before their personal data was shared with third parties and put consumers in control of their data by allowing them to access, correct, and even delete personal data.

But many of the businesses that today complain about the burden of complying with the patchwork of State laws, I have the advantage of having been there then even before Maria Cantwell's bill was introduced when the companies were lobbying against a Federal privacy law, and now they're back complaining about the patchwork of laws. And I would like to change that, but I do think it's important to know that's why we're in the position that we are and to understand why some of these States are looking at this going, "Wait a minute."

The need for Federal privacy reform is even more urgent as AI continues to expand its role into our lives. Data is both the gasoline and the engine for AI models. That means that demand for our data is skyrocketing. So, it is critical that we set guardrails to ensure the data that powers AI is responsibly sourced, and used for legitimate means, and protected when you want to have it protected.

Luckily, there is a bipartisan agreement that Congress needs to act. The Commerce Committee on which Chair Blackburn and I also sit has seen a strong bipartisan, bicameral proposal for Federal privacy reform. Not everyone agrees with all of them, but there has been some start out of that Committee, and I look forward to hearing from our witnesses about why we need these guardrails now.

Thank you, Senator Blackburn.

Chair BLACKBURN. I thank you and our witnesses. Ms. Kate Goodloe is managing director at the Business Software Alliance, where she develops policies on privacy, AI, and law enforcement access. She also taught AI law at the GW Law School. Prior to her time at BSA, Ms. Goodloe was a senior associate at Covington & Burling focusing on privacy and cybersecurity. She earned her JD from the New York University School of Law. We welcome you.

Mr. Joel Thayer is the president of the Digital Progress Institute and founder of Thayer, PLLC. He has represented clients before the FCC, FTC, and Federal courts on issues relating to telecom law, data privacy, cybersecurity, and competition policy.

Before that, he has held positions at the App Association, the FCC, the FTC, and the U.S. House of Representatives. Since earning his JD from American University Washington College of Law, he has been recognized as a Super Lawyers Rising Star for his work in communications law and digital policy.

Mr. Paul Martino is a partner at Hunton Andrews Kurth, LLP. He has nearly 25 years of experience in public policy and government relations specializing in privacy, data security, AI, e-com-

merce, and tech. Mr. Martino is the founder and general counsel of the Main Street Privacy Coalition.

Before joining Hunton, he served as VP and senior policy counsel for the National Retail Federation and co-chaired the Privacy and Data Security Task Force at Alston and Byrd. After earning his JD from the University of California, Berkeley School of Law, he served as Majority counsel on the Senate Commerce Committee for, then Chairman, John McCain.

Alan Butler is the executive director and president of the Electronic Privacy Information Center. Before his role as executive director, he managed EPIC's litigation and amicus program where he filed briefs before the U.S. Supreme Court and other appellate courts in privacy and civil liberties cases. After earning his JD from UCLA School of Law, he was admitted to the DC Bar and the State Bar of California.

Samuel Levine is a senior fellow at the Berkeley Center for Consumer Law and Economic Justice. He previously served as director of the Federal Trade Commission's Bureau of Consumer Protection. Prior to his role at the FTC, Mr. Levine served as an attorney advisor to Commissioner Chopra as an attorney in the FTC's Midwest Regional Office, and as an assistant attorney general in Illinois. After earning his JD from Harvard Law, he clerked on the U.S. District Court for the Northern District of Illinois.

We welcome each of you for being here. Now, I'm going to ask you to rise and raise your right hand.

[Witnesses are sworn in.]

Chair BLACKBURN. And we will note that everyone has answered in the affirmative. Okay. Ms. Goodloe, you are recognized for 5 minutes, and we'll go right down the line.

STATEMENT OF KATE GOODLOE, MANAGING DIRECTOR, BUSINESS SOFTWARE ALLIANCE, WASHINGTON, DC

Ms. GOODLOE. Good afternoon, Chair Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee. My name is Kate Goodloe, I'm managing director at the Business Software Alliance, or BSA.

BSA members create the business-to-business technologies used by companies across industries. Privacy and security are core to our members' operations. I commend the Subcommittee for convening today's hearing, and I thank you for the opportunity to testify. The United States needs a strong, clear, comprehensive consumer privacy law. BSA has been a longtime supporter of adopting a Federal privacy law.

Americans share their personal information online every day, whether we shop online, use apps to track our workouts, take ride shares, or host video calls with friends and family, we provide personal information to a broad range of companies. Consumers deserve to know their data is used responsibly.

In our view, a Federal privacy law should achieve three goals. First, it should require companies to handle consumers' personal data responsibly, and assign obligations to companies based on their role in handling that data. Second, it should give consumers new rights. And third, it should create strong consistent enforcement.

I want to focus on that first goal. To create the right set of obligations, a privacy law must recognize different types of companies handle consumers data. Those companies must all adopt strong but different safeguards to effectively protect consumers. Most importantly, not all companies are consumer-facing.

BSA represents the business-to-business technology providers that work for companies across the economy. An online store that sells clothing for example, will rely on a series of business-to-business technology providers. It may use one to manage customer service inquiries, another to track deliveries, and a third to protect its data against cybersecurity threats.

Each company must protect the personal data it handles, but companies need to take different actions to effectively protect consumers because they play different roles in handling their data. Laws should not create a one-size-fits-all obligation. Treating an online store and its cybersecurity vendor alike doing so actually creates new privacy and security risks for consumers.

Now, this is something that States get right. Twenty States, both red and blue, have adopted comprehensive consumer privacy laws and those laws are remarkably consistent. All 20 reflect a fundamental distinction between two types of companies that handle consumer's data and assign strong but different obligations to each.

The first are controllers. These companies decide how and why to collect a consumer's personal data, and State laws give them obligations about those decisions, including; telling consumers how and why they process data, responding to consumer rights requests, asking for consent to process sensitive personal data, and minimizing the collection and use of data in the first place.

The second type are processors. These companies have a role of handling data on behalf of a controller, and State laws give them a common set of obligations, too. Those include; processing data pursuant to the controller's instructions, entering into a contract with a controller, handling the data confidentially, and giving controller the information it needs to conduct privacy assessments.

These roles reflect the modern economy. They're not unique to State laws and they're not new. The distinction between controllers and processors dates back more than 40 years, and it underpins privacy laws worldwide. It must be part of any Federal privacy law.

In addition to putting obligations on companies, the Federal privacy law should create new rights for consumers and strong consistent enforcement. Here, too, you can look to States. There is widespread agreement on consumer rights. All 20 States give consumers rights to access, delete, and port their personal data. Nineteen, also give a right to correct inaccurate data. States also create similar enforcement mechanisms, with all 20 giving a leading role to the attorney general to enforce privacy violations.

I look forward to discussing consistent aspects of these State laws, but I want to say that consistency may not last. This year, we've seen a striking interest in amending existing laws to revise, expand, and change their protections and new obligations coming through rulemakings.

A Federal law is needed to bring consistency to existing protections and to create broad long-lasting protections for consumers. A

Federal law should not weaken protections already provided by the States, but extend those protections to consumers nationwide.

There is significant common ground between industry and civil society stakeholders on comprehensive Federal privacy protections. We look forward to working with Congress on these issues.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Goodloe appears as a submission for the record.]

Chair BLACKBURN. And well done right at 5 minutes. You get a gold star on that. Mr. Thayer.

STATEMENT OF JOEL THAYER, PRESIDENT, DIGITAL PROGRESS INSTITUTE, WASHINGTON, DC

Mr. THAYER. I'll try to emulate it. Thank you, Chairwoman Blackburn, Ranking Member Klobuchar and esteem Members of this Committee for inviting me to testify and holding this important hearing. My name is Joel Thayer, and I'm the president of the Digital Progress Institute.

It's a think tank based in Washington, DC, focused on promoting bipartisan policies in the tech and telecom space.

Ensuring privacy for all is a founding principle of the institute. And as such, I very much appreciate the Committee's commitment to building out a privacy framework that further assures that the integrity and ownership of our digital selves remains in our domain, not by a company with a domain name.

Although our privacy from our Government is well established, that is unfortunately not the case with respect to companies. With the allure free services, we provide details about our most intimate selves to trillion-dollar tech companies who in turn make enormous profit off the data they collect. They know everything about us; what we like to eat, when we sleep, where we live, where we are, our beliefs, and even our fears. Curiously, though they claim our age confounds them, but let's set that aside for now.

A recent Pew study shows that 73 percent of Americans feel they have limited to no control over how companies use their personal information. And the reality is they don't. We sign privacy policies that are filled with so much legal jargon that it may as well be unintelligible to the average person, and presto, our data is now their data.

The problem is not just they sell our data to third party advertisers, but also to those who use our data to create fake images, curate bias newsfeeds, conduct elaborate scams, and even engage in espionage campaigns. In short, we are not in control, and Americans are right to be concerned. And with the advent of AI, this trend is only going to increase. It's no wonder why 85 percent of people want more privacy protections.

We need government intervention here. The good news is that protecting privacy is a bipartisan issue. Indeed, 20 States across the political spectrum have passed privacy laws, and as evidenced by this hearing, Congress appears poised to address this issue again. We welcome this much needed development.

With that in mind, here are a few high-level suggestions as the Committee evaluates paths forward. First, it's important to define your goals and keep the framework targeted at accomplishing its

goals. One of the primary issues with previous attempts at passing meaningful privacy laws has been that bills attempt to do too much all at once. We have seen the most success in legislation that has clearly articulated goals with targeted solutions.

It's why the institute has supported targeted bipartisan measures such as the Protecting Americans from Foreign Adversary Controlled Applications Act—that's a mouthful—the TAKE IT DOWN Act, the Kids Online Safety Act, the App Store Accountability Act, and Oama just to name a few.

As we have seen in the EU's GDPR, overly sweeping privacy laws have the unintended consequence of entrenching incumbents. The GDPR should be a cautionary tale for the U.S. because it clearly shows that privacy regulations without market guardrails can seriously exacerbate today's competition issues we have with Big Tech.

Second, enforcement matters. In our experience, agency actions or attorney general enforcement are the most effective, whereas a private right of action alone may act more as a carrot as opposed to a stick given these companies' seemingly endless teams of lawyers and budgets.

For instance, the Texas attorney general recently secured a $1.4 billion settlement against Google for violating its privacy law, whereas when consumers sued Apple under California's privacy law, in part for sharing recorded conversations that included personal health information with their physician to medical ad companies, they were only entitled to a meager $95 million. Worse, consumers won't see about a third of that because that's reserved for their lawyers.

Third, the broader the Federal statute, the more important preemption will become. That's because targeted legislation is less likely to run into differing State privacy regimes. Any preemption framework should be clear on what it is preempting and should reserve rights for State attorney general enforcement.

Key areas though ripe for preemption are addressing basic definitions like; what does personal information mean, the creation of data rights. It seems to be unanimous amongst all State privacy laws, and of course, be specific with what data management practice we seek to prohibit. In some, the reality is that if these Big Tech companies cared about user privacy, they would protect it. Frankly, it's in their interest not to. Congress needs to act. Once again, I would like to thank the Subcommittee for allowing me to testify, and I welcome any questions you may have. Two seconds on this one.

[The prepared statement of Mr. Thayer appears as a submission for the record.]

Chair BLACKBURN. There you go. Well done. Mr. Martino, the pressure is on.

[Laughter.]

STATEMENT OF PAUL MARTINO, GENERAL COUNSEL, MAIN STREET PRIVACY COALITION, WASHINGTON, DC

Mr. MARTINO. Thank you, Chair Blackburn, and Ranking Member Klobuchar, for the invitation to be here today. I am Paul Martino, a partner at Hunton Andrews Kurth, here in Washington,

and I serve as the general counsel for the Main Street Privacy Coalition.

Our coalition members represent a broad array of companies that line America's main streets. They interact with consumers each day. They're found in every town, city, and State, providing jobs, supporting our economy, and serving Americans as a vital part of their communities.

Collectively, Main Street businesses directly employ approximately 34 million Americans, and contribute $4.5 trillion to our Nation's GDP. Since 2019, the coalition has supported Federal privacy legislation that would establish a single nationwide law to protect the privacy of all Americans.

Where we sit here on Capitol Hill today, we can travel to two States in 20 minutes by car or metro. Just like many Americans who live in tri-State areas or near State lines, should Americans privacy rights change as they drive from DC into Maryland or Virginia? They do right now, but many don't know that Americans expect their privacy to be protected the same everywhere.

Our coalition members share a strong conviction that a preemptive Federal privacy law will benefit consumers and Main Street businesses alike. It would give consumers confidence that their data will be uniformly protected across America regardless of where they live or choose to do business. And it would provide the certainty Main Street businesses need to lawfully and responsibly use data to better serve their customers online or across State lines.

Establishing a uniform national law that extends consumer privacy rights and consistent privacy rules to all consumers and businesses in America is a core principle for Main Street. I will highlight two more. First, a Federal privacy law should protect consumers comprehensively with equivalent standards for all businesses. A privacy law should empower consumers to control their personal data used by businesses regardless of business type. Likewise, businesses must be permitted to lawfully use data consumers share with them.

To better serve customer needs. To meet these goals, we recommend a Federal privacy law that creates equivalent privacy obligations for all businesses handling consumer data. This would be a change from past Federal privacy bills that narrowed obligations for service providers in Big Tech, telecom, cable, and financial industries, relieving them from the same obligations that apply to Main Street businesses.

For privacy laws to succeed for consumers, it is critical for all entities handling consumer data to secure that data and protect the privacy rights. This is true regardless of the terms used in privacy laws that blur the reality of who actually controls the data. The label "controller" which is applied to every Main Street business that directly serves a customer, can create a false impression about the power of Main Street businesses as they interact with Big Tech service providers.

Main Street companies control their relationship to customers, a responsibility they value, but very few can control how nationwide service providers operate and do business. Powerful Big Tech and ISP service providers require Main Street businesses to sign "take

it or leave it" contracts that dictate the terms of their service. The myth that Big Tech processors merely follow the instructions of the typical Main Street business is not credible. Privacy laws should not permit any industry sector to shift its responsibilities onto another.

Ensuring equivalent data privacy obligations across industry sectors is also inherently pro-consumer. Consumers have the right to expect privacy rules. They can understand, predict, and support that meet their expectations. Congress can pass a law to ensure that all businesses protect consumer's privacy, and processors cannot hide behind labels that make it appear they have no control at all.

Finally, Federal privacy laws should hold accountable all entities handling personal data with the same enforcement mechanisms. This creates an even playing field with proper incentives across industry. The law should encourage compliance to protect consumers more effectively than gotcha lawsuits that threaten Main Street businesses driving to be in compliance. This is why State privacy laws thoughtfully couple government notice with the opportunity to quickly correct or cure mistakes.

Thank you, and I welcome your questions.

[The prepared statement of Mr. Martino appears as a submission for the record.]

Chair BLACKBURN. And you came in with a few seconds on the clock. You're in the lead. All right, Mr. Butler, we're going to see what you can do here.

STATEMENT OF ALAN BUTLER, EXECUTIVE DIRECTOR AND PRESIDENT, ELECTRONIC PRIVACY INFORMATION CENTER, WASHINGTON, DC

Mr. BUTLER. Thank you, Chair Blackburn, and Ranking Member Klobuchar, and Members of the Subcommittee for the opportunity to testify today about the need to better safeguard American's online data.

My name is Alan Butler and I'm the executive director at the Electronic Privacy Information Center. EPIC is an independent, nonprofit research organization established in 1994 to secure the right to privacy in the digital age for all people.

Twenty-five years ago, the Federal Trade Commission issued a report to Congress based on its research of privacy risks in the online marketplace. The takeaway was clear self-regulation does not work, and we need legislation to ensure adequate protection for Americans online.

In the decades since that report, we have seen our digital world expand and develop in amazing ways, but without strong privacy protections. We have seen an alarming expansion of surveillance and data abuses online that threaten our rights and subvert our most fundamental values of autonomy and freedom.

The status quo is untenable. If the law allows a company to scrape images of all of us to build a universal facial recognition data base, while another company tracks every site we visit to build invasive profiles, and yet another company buys and sells our logs of daily movements, do we have privacy protection at all? I be-

lieve any reasonable person would say no, and would demand that our lawmakers step in to fix this broken system.

In my testimony today, I will describe the current state of State privacy law and identify the areas where Federal leadership would be most impactful. Privacy is a fundamental right and Americans deserve a law that actually protects our data. In the absence of action by Congress, States have stepped in to advance digital rights in the information age. This has been an important catalyst for change, but there's more work ahead to establish robust privacy standards.

There is significant bipartisan agreement across party and State lines about the need for privacy protection in the core principles that should shape the law. So, our attention at the Federal level should be on establishing clear rules of the road to make our digital world safer and more secure. What we cannot do is pass a weak Federal standard that prevents States from responding to new challenges and emerging threats in the future.

A Federal privacy law should set a consistent and robust standard for protection while preserving flexibility for States in the future. Over the past 7 years, 19 States have passed comprehensive data privacy laws and many States have also passed bills aimed at preventing specific privacy harms. Most of these State laws follow a common framework, and have many of the key components of any modern privacy law.

But unfortunately, these laws do very little to actually limit abusive data practices and to protect privacy. In a recent report, EPIC analyzed these laws in detail and graded each of them. Eight received Fs, and none received an A.

So, what went wrong? The tech industry has invested heavily in State lobbying to water down the substantive protections, narrow their scope and add exceptions that swallow the rules. But over the last 2 years, we have seen stronger State proposals building off the bipartisan framework that Congress created in 2019 and 2021.

The Maryland Online Data Privacy Act, for example, passed last year, it builds on existing State laws and incorporates strong data minimization protections, and a ban on the sale of sensitive data. Inspired by Maryland's success, 10 States have introduced bills with strong data minimization rules this year. Several States that originally passed weak privacy laws have revisited and amended their laws to strengthen their protection.

Any Federal privacy proposal should have a strong data minimization rule, include heightened protections for sensitive data, and establish robust enforcement mechanisms. Data minimization offers a practical solution to our broken internet ecosystem. Instead of allowing data collectors to dictate privacy terms, data minimization rules set clear standards to limit the processing of our data. Companies can collect the data they need to provide the services we want. This standard better aligns business' conduct with what consumers expect and stops abusive data practices like third-party tracking and profiling.

Enhanced protections can also ensure that our most sensitive data remains confidential and secure. So, much information about us that has traditionally remained private is now captured in digital form; our health records, our movements, our biometrics, and

genetic markers, even the data about our children. These records are frequently targeted by hackers and scammers, and should be locked down and secure.

Strong privacy standards should also be backed up by robust enforcement, including the three-tiered approach that we saw in the Federal bill. And while State and Federal enforcement is essential, the scope of data collection online is simply too vast for any one entity to regulate, and that is why private rights of action with enforceable court orders are so important.

EPIC has been calling on Congress to pass a strong privacy law to protect all Americans for the past 25 years. We are grateful that the Subcommittee is turning its attention to this important issue, and we urge Federal lawmakers to learn from State's experience.

I thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Martino appears as a submission for the record.]

Chair BLACKBURN. And Mr. Levine, you're recognized.

STATEMENT OF SAMUEL LEVINE, SENIOR FELLOW, UC BERKELEY CENTER FOR CONSUMER LAW & ECONOMIC JUSTICE, NEW YORK, NEW YORK

Mr. LEVINE. Thank you, Senator. My name is Sam Levine, and I'm a senior fellow at Berkeley Center for Consumer Law and Economic Justice. Until January, I led the FTC's Bureau of Consumer Protection.

Today, protecting Americans' personal information is about much more than privacy. It's about whether we can afford essential goods, whether we can be profiled based on our political or religious beliefs, and whether the next generation will grow up addicted to screens. I'll be focusing on three real-world threats that unchecked privacy abuses are fueling threats to economic fairness, democratic freedoms, and the safety of kids and teens.

Let's start with economic fairness. On a recent earnings call, Delta Airlines executives boasted they could soon raise prices on plane tickets, not by adding value, but through a new formula; stop matching competitors' prices, unbundle basic services and charge each passenger the most they're willing to pay.

Investors cheered the news calling this the Holy Grail, but we should call it what it is; personalized price gouging. And it's only possible because weak privacy protections are allowing companies to track our behavior and predict how much we can be pushed to pay.

This practice, also known as surveillance pricing, is spreading. More and more businesses are looking to price everyday goods from groceries to hardware the way airlines are pricing tickets. And let's be clear, their goal is not to lower prices, it's to charge each person as much as possible and the people hit hardest will be those with the fewest options; a parent buying baby formula, a senior filling a prescription, or family booking last minute travel to a funeral.

Unchecked data collection is moving us from a world of one product, one price, to one person, one price. And if we don't act, the shift will be costly. Uncheck data collection is also putting our democratic freedoms at risk. Last year, the Federal Government al-

leged that an entity was tracking American's movements and profiling them into categories like Wisconsin Christian churchgoers, likely Republican voters, and restaurant visitor during COVID quarantine.

This was not a foreign adversary. This was a U.S. data broker. The FTC sued to halt these practices. That lawsuit should be a wakeup call. No American should be profiled based on their politics, their religion, or their stance on COVID lockdowns. Yet, without strong data protections, that's exactly what brokers are doing. Political and religious freedom cannot thrive in a society where our movements, beliefs, and behaviors are tracked, recorded, and then sold to the highest bidder.

We need to act. We also need to act to protect our next generation. Over the past two decades, Big Tech has been running a massive experiment on our children; what excites them, what enrages them, and what holds their attention? The result is a youth mental health crisis.

Weak data privacy is powering these harms. Social media companies collect personal data to power their ad-driven business models. More screen time means more revenue, and more insights into how to keep kids hooked. It's a dangerous feedback loop that profits from addiction and it's getting worse.

Today, companies are building AI chatbots engineered to earn kids' trust and keep them engaged. And that means serving up content that's provocative, obscene, and sometimes dangerous. One bot reportedly told a teen that self-harm feels good. Another offered lesson on how kids can hide drugs and alcohol, and how to set the mood for sex with an adult.

You might expect these incidents to prompt a pause, but the opposite is happening. The same tech giants that have been putting kids at risk for years are now racing to roll out AI chatbots, and respectfully, they are doing so because Congress is not telling them they need to stop. That must change across each of these threats.

The common thread is weak data protection, but we can fight back. Strong privacy laws can stop companies from using personal data to set individualized prices, ban the profiling of Americans based on sensitive information, and end the surveillance that's fueling an endless cycle of harm to kids and teens.

Thank you for holding this important hearing today, and I look forward to taking your questions.

[The prepared statement of Mr. Levine appears as a submission for the record.]

Chair BLACKBURN. And you win the gold medal.

Mr. LEVINE. Thank you.

Chair BLACKBURN. Yes. I think it was 23 seconds left. We're going to move to questions, and Senator Klobuchar, I will let you begin.

Senator KLOBUCHAR. Okay, very good. Thank you very much. So, as I discussed earlier, there've been a number of bipartisan proposals for Federal data privacy law that have been introduced over the years, including the American Privacy Rights Act, and the American Data Privacy and Protection Act.

I guess, Mr. Butler, I will start with you. Why is it so essential that we put reforms like these in place for consumers across the country?

Mr. BUTLER. Well, thank you for the question, Senator Klobuchar. I mean, we've seen what happens without Federal leadership on privacy. Surveillance tools have become embedded in every website and app that we visit. And without a Federal standard, companies really don't have the incentive to innovate on privacy protection and a few Big Tech firms dominate the marketplace.

So, we're fueling harms to individuals, we're fueling harms to the market, and we're just allowing ourselves to be inundated by these surveillance and abusive data collection practices.

Senator KLOBUCHAR. Thank you. And Ms. Goodloe, in your testimony, you highlight that there's broad consensus on many privacy principles across the 20 States that have them both Democratic- and Republican-led. I think Mr. Butler was mentioning how some of the early laws were weaker. There have been some improvements. What are the significant areas of bipartisan consensus that should be at the core of Federal privacy legislation?

Ms. GOODLOE. Thank you for the question. We see a lot of consensus on the right set of rights to give to consumers both affirmative rights like the ability to access, correct, and delete their information, and on giving them rights to opt out of certain activities, including the sale of their data profiling and targeted advertising. I think there is consensus among many most of these State privacy laws on that set of important issues.

There's also a core set of obligations on companies for controllers. It's things like asking for consent to process sensitive data. We have 17 States that require companies that are processing sensitive data to conduct privacy assessments, looking at the sensitive issues arising from that processing.

And when it comes to processors, there is broad consensus that they have a separate set of rights to handle data on behalf of a controller pursuant to their instructions and to do so confidentially.

Senator KLOBUCHAR. Okay, thank you. Mr. Levine, while at the FTC, you prosecuted unfair and deceptive acts and practices related to data privacy, as well as other privacy laws like those intended to pre protect young children.

Despite your efforts to use every legal tool at your disposal to protect privacy, what gaps exist that are the most critical for Congress to fill through a comprehensive data privacy bill?

Mr. LEVINE. Well, thank you for the question, Senator. And as you alluded to in your remarks, we currently live under a privacy regime where companies have taken the position that they can basically do whatever they want so long as they disclose it in their privacy policy.

Over the last 4 years, the FTC, we took a number of steps to try to push back against that. We told GoodRx they couldn't share sensitive medication information with Facebook even if consumers clicked "Yes." We told Better Health they couldn't share with advertisers what mental health treatments people were seeking. We told Amazon Ring that its employees couldn't spy on people who were using their security cameras.

But I can tell you, Senator, that every case we brought, when I would meet with counsel for those companies, they would tell us the same thing, "Well, we put it in our privacy policy, so it's legal."

I think our enforcement, the FTC's enforcement, and State enforcement, and privacy enforcement would be far more effective with bright-line rules on what companies can collect, how they can use it, and with whom they can be shared. Without that, you're going to continue to see a whack-a-mole approach that doesn't do enough to protect Americans' privacy.

Senator KLOBUCHAR. Thank you. Very good. Mr. Thayer, I've long advocated for common-sense rules to require the platforms to allow competing businesses the same access to the platform that they give themselves. Senator Blackburn has advocated for similar reforms in app store markets, but as you mentioned in your testimony, dominant platforms use privacy concerns as a pretext to avoid opening up their platforms to fair competition.

How can interoperability requirements be implemented without putting user privacy at risk?

Mr. THAYER. Thank you for the question, Senator, and also thank you for your work that you do on this. And also, Senator Blackburn, you guys have been real champions on this issue, and I think it really does highlight the significant aspects in the concentration that this market involves, where we have basically four players, maybe three in some markets, or maybe even two in others, particularly an app store where you really have—you're at the behest of or at the whim of whatever these companies want you to do. So, you're basically stuck with whatever privacy policies that they decide on.

And so, a good example of this is the software we're seeing at the DOJ, with AG Gail Slater at the helm, where she's been arguing on the remedies case. And the first argument that you got from Google was like, "Hey, you can't do this sharing arrangement because it'll violate privacy." But in reality, what they really care about is scale. They want to harbor the data. They don't really care about the privacy at all. It's really all a ruse.

Senator KLOBUCHAR. And how can a strong Federal privacy law help ensure that interoperability opens up digital markets to competition?

Mr. THAYER. So, I really point to the idea of a general statute versus a specific statute. And as you know, Senator, the antitrust laws are pretty broad, and so are Section 5 of the FTC Act. Being able to designate exactly what we're interested in and target the actual acts that we're concerned with will help regulators down the road.

And this is precisely what Mr. Levine was alluding to when bringing that broader framework out. If we say interop is something that we all believe is something that could equal out or balance out the scales, then it gives the regulator the ability to assess it in that way instead of using vague statutes.

Senator KLOBUCHAR. Okay. Last question, Mr. Martino. As you know, I was close friends of John McCain, and miss him very much. In your written testimony, you say that businesses should not be responsible for the data privacy practices of other entities whose actions they cannot control, including the Big Tech plat-

forms on which we know many businesses now have to rely to reach consumers.

How can Congress ensure that responsibility is aligned properly with the entities best suited to protect consumer privacy?

Mr. MARTINO. Thank you, Senator Klobuchar. Well, I think the core principle we have here is that businesses need to have equivalent requirements, equivalent standards to protect data. There's a chart in my testimony that——

Senator KLOBUCHAR. You like charts, huh?

Mr. MARTINO. Yes, I like charts [holds up documents]. I didn't make it real big though, [laughter]. Sorry. But it's it shows some of the State law requirements for the Big Tech service providers. And you'll notice there are a couple red Xs here on things that I think consumers would expect and businesses like Main Street businesses would expect their service providers to do which is provide data security.

The State laws for the most part, except for Colorado, I believe, don't require the Big Tech service providers to actually secure the data they're processing on behalf of businesses. They're only required to assist the controllers in their own data security and if they have their own breach, but there's a lack of parity there.

Another place that I'll mention where there's a red X and again, you know, only I think Colorado and Connecticut have done this, but processors use lots of subprocessors or subcontractors, and they have requirements that any subprocessors they share the data with has to meet the same standards as the processor.

But, you know, they don't give the Main Street business an opportunity to object to those subprocessors, to those subcontractors. Only in two States that I'm aware of. And that is a big difference between, for example, what happens in Europe and what happens in the U.S. And so, if you have a processor that you don't want to downstream pass on data to—you know, think of some of the past breaches and privacy violations we've seen before, you know, the Main Street business should have the ability to object to that. So, we ask for the similar requirements that Main Street businesses have to live by.

Senator KLOBUCHAR. Okay. Thanks. And thank you. Sorry to go over.

Chair BLACKBURN. No, thank you. It is perfectly fine that you went over. This is the first of our hearings that are going to look at this virtual space. And as you all know, Senator Klobuchar, and I've done a lot of work and trying to secure the American citizens' privacy in the virtual space.

And as we work through this on this Committee, I think that foundational to the conversations is who owns an internet user's data and what is the scope of that ownership? Where does it begin? Where does it end? And let's just go down the line, Ms. Goodloe, starting with you, and everybody keep it under a minute and answer that question so that we've got that for the record.

Ms. GOODLOE. Thank you for the question. Our companies provide business-to-business technologies to other companies. In many cases, their business customers own the data that they store with business-to-business providers, and yet there may be personal data that individuals own as well.

And those individuals should have rights like to access, correct, and delete that information no matter whether it's stored with a consumer-facing company or the business-to-business provider processing it on behalf of that consumer-facing company.

Chair BLACKBURN. Okay. Mr. Thayer?

Mr. THAYER. Given the lack of appropriate consent to regimes, I would say that the user owns that data, because I don't think that the way we have things set up right now the data subject, doesn't even know that they've given over some of that data.

And so, at the end of the day, I think the reality is that we have to have privacy regimes in place to ensure that the ownership to outline those particular contours. But it is 100 percent you own your data, and it shouldn't be the other way around.

Chair BLACKBURN. Okay.

Mr. MARTINO. Thank you, Senator, for your question. It's a very good question. There are some nuances here I think that are important. First, Main Street businesses understand it's the user's data and the user has the right to correct it, delete it, remove it from their system. But there are some kinds of data that is considered shared.

And so, for example, if you make a purchase in a store, well, the store needs to keep a record of that purchase if you want to do a return or an exchange for their inventory. So, is it the consumers'—that this consumer made this purchase on this date? Is that personal information? Yes. Is it also information the business needs and can't just get rid of? Yes.

And so, I think when it comes down to ownership, we just have to understand that in modern commerce and e-commerce, some information will need to be retained, but only for as long as it's necessary to retain it. And I think hopefully that answers the question.

Chair BLACKBURN. Okay.

Mr. BUTLER. Thank you for the question, Chair Blackburn. We believe that we all have a fundamental right to control when our data is used and how it is collected. But individual mechanisms of consent and control don't provide a complete solution to this problem, and that's why we feel that it is so important to have rules of the road that protect people's privacy by default and align business collection and use data practices with what consumers reasonably expect.

Chair BLACKBURN. Okay.

Mr. LEVINE. Thank you, Senator. I very much agree with Mr. Butler. Data about people should be owned by people, but at the same time, as Alan said, we don't want a world in which people are solely responsible for protecting their own privacy. That's why we need strong Federal protections that don't put the onus on people, but put the onus on companies to make sure they're not abusing people's privacy.

Chair BLACKBURN. Yes. It was over a decade ago that now Senator Welch and I were in the House at Energy and Commerce Committee—I know Mr. Martino remembers all of this—and we had bipartisan legislation to establish a data privacy framework. And of course, Big Tech fought it just all the way to today. We still don't have it into law.

So, Mr. Thayer, talk for a minute about why Big Tech has found it so vitally important to kill any effort to have Federal online privacy?

Mr. THAYER. Because it's against their financial interest to actually be regulated. I mean, that's the basic—that's the obvious answer, but in reality, what you're pointing out, and I think everyone on this Subcommittee has experienced, it doesn't matter how tailored you make your legislation, it doesn't matter how measured. They will find some reason and put something forward.

If you want to do any trust reform, for instance, they'll say there's a privacy violation. If you say there's privacy, then we don't have to worry about competition. It's always this game of Whack-a-Mole. And so, at the end of the day, they like the way things are because it benefits them. The market is basically created for them.

And so, I think this is exactly why we have strong advocates fighting for things like the Kids' Online Safety Act, where you have parents begging Congress to do something, and we're seeing the harms play out right in front of us. I think at this point, we've recognized that Big Tech is in the "emperor has no pants" moment and we are all starting to see that; that we absolutely need the reforms.

And so, things like the Open App Markets Act are going to be very helpful to quell any of those privacy concerns. The Kids Online Safety Act, I think will do really do a lot to measure targeted approaches that will ultimately help kids. But again, I think that the waves are changing, and I think that there—I'm very hopeful, and things that I'm seeing at the DOJ, especially from the Trump administration to the Biden administration out the gate to the new Trump administration, it seems as if everyone has identified that these companies are bad actors and they should not be trusted.

So, I hope whatever advocacy I can provide would be to outline that this really just don't fall for the red herrings. Ultimately, the side of right is to protect consumers, and Big Tech has no interest in doing that.

Chair BLACKBURN. Ms. Goodloe, I want to come back to you. In your testimony, you talked about State laws and the importance of some of those State laws. I want you to define a couple of the common elements that you have seen in the State laws that could be transferred into a Federal law that should be broadly supported and accepted.

Ms. GOODLOE. Thank you for the question. I think the States provide a lot of common ground for Congress to look to as it works toward Federal privacy legislation. That common ground exists on things like the consumer rights that we've talked about today, rights to access, correct, delete, and port your data to another service, rights to opt out of the sale of your data, targeted advertising, certain types of profiling.

And States are unanimous on recognizing there are different types of companies that handle consumers' data. One set of obligations should be assigned to controllers who decide how and why to collect a consumer's data, how to use it. And one set of obligations should be put on the processors that handle the data on behalf of controllers.

I also want to take a moment to respond to something that Mr. Martino brought up about what those processors do when they employ other subprocessors. Because in many cases, what processors do is they collect a series of other subprocessors, package it together, and are able to provide it to business customers at scale so that their small businesses can enjoy the economies of scale at being able to use cutting edge technologies.

That means you are providing the same service to hundreds or thousands of business customers. And letting one object to a package of subprocessor doesn't work. That's why we haven't seen the majority of States adopt that, which could actually increase security risk to consumers when one of those subprocessors has a breach and they have to go and ask permission to change over the data.

But I think we do see broad agreement among the States about the right set of consumer rights and obligations on businesses to safeguard consumers' data, and to do so effectively along with a common enforcement system that is a regulatory-led enforcement system to ensure we have consistent expectations for companies that want to comply with privacy and security obligations.

Chair BLACKBURN. Mr. Martino, you wanted to respond?

Mr. MARTINO. Yes. Just on the point. And one thing to keep in mind with the ADPPA, that was the predecessor to the APRA. The way the definitions worked, a subprocessor was also defined as a processor. So, once it got to a processor, there could be this endless train of data sharing that the mainstream business has no control over.

Well, that might be great for efficiencies of the services that the main processor is providing. You know there's no check on the downstream. And so, that's why all that we've been pushing for was a simple notice to the Main Street business of the subprocessor you are using and the right to object. It's not like an opt-in that they can't go to them and they can't provide these efficiencies.

So, that's just a—I mean, it's an "in the weeds" point. But I think it's an important point because it's the Main Street businesses that will be held liable under most of these constructs because the same requirements aren't applying to the processors and the same enforcement mechanisms aren't applying.

I'll make one last point. In the APRA, the private right of action largely applied only to what are called the "controllers", but of course, these Main Street businesses that can't really control the Big Tech companies. And it hardly applied to the processors and it didn't apply at all to the third parties.

So, I think we have to look at not just that these State laws have requirements, but who's subject to them and who's liable for those violations.

Chair BLACKBURN. Okay. You had additional questions?

Senator KLOBUCHAR. Yes.

Chair BLACKBURN. Go ahead.

Senator KLOBUCHAR. It's really an extraordinary panel, so thank you. I guess I would start with you again, Mr. Butler. Over time we've seen that these data privacy frameworks move away from a notice and consent regime to focus on data minimization and trans-

parency, consumer control opt-out rights. Why is notice and consent insufficient for protecting user privacy?

Mr. BUTLER. Thank you for the question, Senator Klobuchar. I think, notice and consent really takes us back to that self-regulation point that was made in the FTC report 25 years ago, because that's essentially what it is, right? It's a rule set that says so long as you disclose in general terms what you're doing, then the law permits it.

And of course, the incentives there are clear, you put in your disclosure everything you could ever potentially——

Senator KLOBUCHAR. That I never read.

Mr. BUTLER [continuing]. Do with that data——

Senator KLOBUCHAR. Says the Senator who decided every morning this week I'm going to spend 5 minutes pushing "unsubscribe" on my email, and I am still getting—I cut it in half what I'm getting. Yes, it's a nightmare.

Mr. BUTLER. And it doesn't shift business practices.

Senator KLOBUCHAR. I know, but it's just really sad. Okay. Continue on, Mr. Butler.

Mr. BUTLER. And it doesn't shift business practices, and it doesn't change anything about the surveillance that surrounds us and the data collection that pervades, which is why a data set of data minimization rules that better align the business practices with the expectations of the users, and link the collection and use of data to what the services that people are actually requesting, I think better aligns with those reasons, and is much a much easier way to solve the problem.

Then, as I mentioned earlier, the individual control concept, which then requires us to all make thousands of choices every second of every day and face popups and questions in detailed settings.

Senator KLOBUCHAR. Right. And then you pop the wrong one, suddenly you're in something else.

Mr. BUTLER. Exactly.

Senator KLOBUCHAR. Mr. Levine what barriers does today's notice and consent, a regime that I was just talking to Mr. Butler about for data privacy, create for enforcers who are trying to protect consumers?

Mr. LEVINE. That's a great question, Senator, and I alluded to it earlier. It's not only are data privacy cases, but so many of the enforcement actions we brought at the FTC over the last 4 years, we said, "Look, you surprised consumers. You misled consumers. You abused their data. You shared what medication they were taking with Facebook." And the company says, "Hold up. We put it all in our privacy policy, and the consumer clicked, 'I accept,' before proceeding to use the service." This is a total fiction. It's a total fantasy that consumers can protect themselves by reading privacy policies.

And to Mr. Thayer's excellent point, we can draw a direct line between Congress', in my opinion, inability to pass privacy laws and Big Tech lobbying. This is the most valuable industry in the history of the planet, and they have built their revenue not by selling cars, not by selling oil, but by collecting our data and predicting our behaviors. That's how they've built their valuations. They don't

want restrictions in what they can collect, and that's why I think it's so important Congress defy what they want and actually pass a strong bill.

Senator KLOBUCHAR. Very good. Mr. Martino, in your written testimony, you say that businesses should not be responsible for the data practices. We already went over that, but I guess my second question about that is just when you look at the differences between—as we look at how we craft this Federal law, and the States, and what's stopped us before, well, how do you think we're going to get around that to get to a place where we can get something done?

Mr. MARTINO. That's a great question. Thank you, Senator. I do think that we start with where the strong consensus of State laws have been. They have outlined, as Ms. Goodloe pointed out, a set of requirements. Our issue has really been with who gets exemptions, who's subject to the liability for violations, and is the law taking care of it?

I would say one of the things you can take from the State laws is that they realize there is this imbalance in negotiating power between smaller Main Street businesses and large Big Tech companies. So, they have taken the route of putting statutory requirements in.

We're just asking that you build on that framework and add a few more. One of the key issues on the APRA and the ADPPA before it was—that on there was a big debate over data minimization standards. And when the bill was originally drafted, the ADPPA, it was applying to both covered entities which are like the controllers or Main Street businesses as well as the processors.

But processors and Big Tech did not support that bill until that data minimization standard was changed to apply only to covered entities or controllers, and that is a fundamental difference.

I think while there are very good requirements in State levels. And most of the States from the same place it is not the case that everyone in the marketplace is handling data and protecting data for consumers and honoring their rights to the same level that is being put on the consumer-facing businesses. And we think Americans expect that their privacy is the same everywhere, as I said in my testimony. And we should have requirements that make that happen.

In terms of the politics, you know, if Big Tech's been fighting some of the previous bills that weren't so heavy on them, it's going to be more challenging if bills are more fairly and have equivalent standards more fairly balanced so but.

Senator KLOBUCHAR. One of our best arguments as we look at the politics of this is on both sides is affordability. And Mr. Levine, I know you did this study on how the collection of this data can affect affordability. So, I look at some of the fresh, new arguments we can make to convince our colleagues, which is always fun to do, but we're doing better and better. Could you tell us about that?

Mr. LEVINE. Well, I think it is a new argument, Senator, because it's a new practice. We're seeing more and more companies using—some people think of privacy as a discrete issue; I have nothing to hide, you have nothing to hide. Privacy is much deeper than that. And what we are finding and what the FTC study found is that

companies are using these reams of data as they've collected. And they've historically used to target people with advertisements.

We know that's been very profitable, but they're suddenly realizing they could target people with individual prices. And they go around and they tell Members of Congress and State houses, "Oh, we're just doing this because we want to lower prices and send people discounts."

This is ridiculous. They are paying companies like McKinsey, high pricing consultants, to use AI optimization and reams of consumer data to set individual prices. And they're not doing it to lower their profits. They're not doing it to lower their prices. They're doing it so that they can raise prices on the Americans who are most desperate for goods and services.

We have always seen that pricing abuses can start in the airline industry. That is what we are seeing now with Delta, and I have a lot of concern this is going to spread throughout the economy, and the early results of our FTC study show that it already is.

Senator KLOBUCHAR. And we've seen the same thing with rent, by the way——

Mr. LEVINE. Absolutely.

Senator KLOBUCHAR [continuing]. Collecting of data on rent.

Chair BLACKBURN. Let me jump in on this, because we really appreciate having all of you here. On surveillance pricing. Just a show of hands, do you think surveillance pricing should be banned?

[Hands raised.]

Mr. LEVINE. Yes.

Chair BLACKBURN. Okay.

Mr. THAYER. How would you define surveillance pricing?

Chair BLACKBURN. I know, I know. I just wanted a response. Mr. Martino?

Mr. MARTINO. For the record, my hand was not up, it was down—asking a question as to what you meant, but yes.

Chair BLACKBURN. I want you to talk then a little bit about shared data, order, history, loyalty programs, and then how long you keep that, and how you incent that keeping of the data because that's a choice that somebody makes to enter into that loyalty program.

Mr. MARTINO. Absolutely, Senator, and in doing so, let me just first address what Mr. Levine said. I know there's the concern that what pricing may happen in one industry, or the way those practices go, it may come down to retail.

I think there's a very significant difference between the retail industry and let's say some other industries. And it's really comes down to competition where you have robust competition like you do in the retail industry and very low profit margins. The goal on retail is volume. It's business. It's attracting new customers. It's growing the business because you have very little profit on each item.

And what that leads to is, I think, a market constraint. So, almost like a defacto regulation in terms of having such severe competition that your competitor is one click or tap away on an app or one stop away. And so, what's the mindset of retailers and Main Street businesses is how do I attract more customers? How do I do that?

Well, you have to do that with excellent customer service. I mean, the only way to really differentiate yourself is to do that. And so, loyalty plans are one way that is done. There's a report that I cited to in the testimony called the Bond Brand Loyalty Report. They do it every year. They've been doing it the last 14 or 15 years.

They survey consumers, consumers say that 85 percent of them will continue to shop at a brand if they have a great, or, or yes, will continue to buy products from a brand that has a great loyalty program. So, yes, loyalty programs are one of those very important features.

And also, it's important to note, it's also inherently privacy, protective of loyalty plan in the sense that they're not foisted on consumers without their choice. You have to opt in to avoid a loyalty program. You have to be delivered the deal and decide whether you want to do that or not. And the State laws recognize this as well.

The only protections for loyalty plans are based on bonafide loyalty plans where a consumer has voluntarily opted into participate in it. So, I think there are ways that, you know, one of our principles is that businesses and consumers should be able to freely develop a business relationship.

And if businesses on Main Street can develop those relationships, whether it's a very small business offering a buy one get two free, or buy five cups of coffee, get the six one free, they should be able to have those kinds of relationships as long as they're privacy protective. And we think they are in terms of making sure they're voluntary.

And it's important to also note that the loyalty programs are subject in the State laws to every other requirement in the law. So, whether it's a right to opt out or a right to delete, the consumers have those rights. So, we think there are good business ways to do it.

And loyalty is something that's been around in the retail industry for centuries. And we could go to general store examples and things from 1890, but the same thing applied back then that applies now.

Chair BLACKBURN. Okay. Mr. Levine?

Mr. LEVINE. Well, thank you, Senator. You know, it's one thing to join a loyalty program and say you can track my purchase history in exchange for getting coupons, fine, but what the FTC study showed is that these consultants are telling companies; look at what consumers are Googling, look at what they're searching online, look at their location, look at how they're sorting products.

A bunch of California law enforcers actually sued Target for increasing in-app prices while consumers were inside a Target store. So, they didn't know that they could pay lower prices when they're not at the store.

Briefly, with respect to loyalty programs, again, I think if consumers voluntarily turn over information, that's fine. But what we saw in this Delta earnings call is what Delta said is we can stop matching prices because of our brand strength, because of our customers' loyalty.

And in a world of surveillance pricing, my fear is that companies are going to prey on the consumers who are going to pay the most.

You might say they're the most loyal, rather than giving them discounts. That's what we're already seeing in the airline industry.

Chair BLACKBURN. All right. Mr. Martino, come back?

Mr. MARTINO. I'll keep it to a 10-second response. What applies to Delta doesn't apply to Main Street businesses. You have to look at the size of the market, the competition in the market. Airline industry is notorious for being very few competitors, not millions of businesses across America.

Chair BLACKBURN. Years ago, as we were starting in on this debate, I would have people take out their key chain and look at their fobs that were on there, and those are programs they were choosing to share information with because of the incentive that would come back to them.

Those times have changed. I want to go to the issue of AI because we are looking at these AI models that are collecting more and more personal data. They are doing tracking search history monitoring. And as we look at the prevalence of AI, and we've had a hearing on the NO FAKES Act to protect name, image, likeness, and voice of individuals, and that in essence is a form of privacy.

But one of the questions that will come before us as we look at developing a Federal privacy standard is how you hit that sweet spot of being strict enough to have that preemptive Federal enforcement, but yet, flexible enough to allow the innovation of new technologies that we see, things that are going to run on quantum rails, things that are going to be AI applications.

So, Ms. Goodloe, let me come to you on that, and then I'd like Mr. Thayer for you to give me a response also.

Ms. GOODLOE. This is such an important question, and thank you for asking that. I think there are a couple of different ways to look at the need for a Federal privacy law and its intersection with AI technologies. I think the first thing to look at is a recognition that AI can involve many different types of data. Some of that data may be personal if an AI system is using personal data that relates to consumers. But a lot of the data used to train AI systems is not personal data. For example, AI systems may be trained to detect weather patterns based on data that's just about the weather and not about people. But when it comes to AI systems that may be processing personal data, that's where a Federal privacy law is very important to create the right set of safeguards so that consumers know their data will be handled responsibly in, trustworthy ways.

One key issue is exactly what you pointed out, the need to make sure that a law is flexible enough to allow those products to continue to innovate over time. And I think this is one of the struggles that we've seen as the conversation about data minimization has evolved. That is such an important conversation, but you have to get it right because a standard needs to allow for technologies to get better over time. I expect all of the technology that I use today to be better next year and even better the year after that. And so, it is important as you look at these protections to make sure they're flexible over time and to think through the uses that you want to apply to create the right set of safeguards.

Chair BLACKBURN. Okay. Mr. Thayer?

Mr. THAYER. Thank you, Senator. And I think Kate put it very well. There is that nuance when it comes to AI, right? You do have that anonymized data, but there also is the question of what the consumer expected when they gave that data over. And I failed to remember exactly who said it, but it really is like big that data is the new oil and what runs the machine.

The AI machine is data. So, the question is where are they getting it and how are they using it? So, I think at the front end, the consumer has to know how is this data going to be used? Is it going to be used to train an AI system? Are there elements of transparency in terms of how this this this data is going to be used down the road?

That comes down to really being upfront with the consumer on where the data is going. And I think that's when it goes back to my testimony when I said that we just feel like it's out of control. We don't feel like we know exactly what happens when we put the data into any application or any use of search. So, a big part of this is going to be transparency, and specifically, what data these AI systems are training on. Are they training on PII, are they training on anonymized data? Where are they pulling it?

And Senator, as you well know, there are ancillary issues like intellectual property that are also included into all of this as well. So, the big question really comes down to, with respect to privacy, is what rights do citizens have when it comes to protecting their data on the front end? So, that way, it's not used on the back end to do all the parade of horribles that we've already heard about today.

So, that's how I see it in most cases. I think at the end of the day, the consumer has to know exactly what their data is going to be used, and whether or not it—and also on the AI system, what are they training their data on?

Chair BLACKBURN. So, you're looking for specificity in that utilization?

Mr. THAYER. Specificity, and at the very least, being able to have the consumer be empowered to say, I do not want my data to be used for X, Y, and Z. So, it's both.

Chair BLACKBURN. Opt-in, opt-out.

Mr. THAYER. Yes.

Chair BLACKBURN. All right. Do you have any other——

Senator KLOBUCHAR. Oh, I'll just—I think Senator Schiff is coming. I thought maybe, you know, since we have a glass ceiling for only women asking questions here.

Chair BLACKBURN. We kind of like that.

Senator KLOBUCHAR. I mean, Hawley came by, Blumenthal. They've all had other hearings. They're great, and been really helpful to us. Maybe I'll just ask two more and see if he can make it.

Chair BLACKBURN. Okay. Go ahead.

Senator KLOBUCHAR. So, Mr. Thayer, in your written testimony you referenced a European study that found that after the passage of GDPR, the General Data Protection Regulation——

Chair BLACKBURN. I'm going to have to jump in here because they need me to go to VA to vote.

Senator KLOBUCHAR. That's where he is.

Chair BLACKBURN. Yes, that's where Senator Blumenthal is. So, I will say my thank yous to you-all, in case I don't get back before

this closes, and remind you all that we're going to have questions for the record.

As you can see, we have lots of questions, and we are ever so grateful that you-all have come before us. I'll go vote.

Senator KLOBUCHAR [presiding]. Okay. Thank you very much. And thank you, again, for putting together this hearing.

So, I was talking about the GDPR. We know we don't like everything that Europeans are doing on tech, but there are some good examples of some good things they've done. What about GDPR? Were Big Tech platforms able to take advantage of to entrench their position, and how can we avoid doing the same in the U.S., and how can we design data privacy standards that reign in abuses? What's the good things we can get out of that? I know there's things we could simply do here that they agreed to in Europe that we're still fighting out over here.

Mr. THAYER. So, it's a fantastic question, and I think it really comes down to defining your goals. That was like the first big issue. But in terms of what happened with the GDPR, and to be clear, there are elements of the GDPR that I think a lot of States have latched onto, particularly Texas, where they pull this analytical framework between data controllers and data processors. Being able to articulate exactly who has the responsibility is a big part of it.

Senator KLOBUCHAR. I just want to have the record reflect the Texas used the European model, but keep going.

[Laughter.]

Mr. THAYER. I fell right into it. But I think where things went a little bit awry, where there was this weird responsibility that the controllers basically had with respect to contractual regulation. I think it's Article 24 of the GDPR where the controller basically has to dictate specifically. Well first whether or not they have to make the assessment of whether or not the processor is even GDPR compliant. And that gives the controller a lot of authority over what that smaller company most likely can do and can't do. I think that's one area we may want to stay away from.

But my overall point was that you need privacy and strong antitrust enforcement in competition enforcement. I think the both two things go hand in hand. And so, I think what Congress is currently looking at and I think is very important is that it seems like you guys want to walk and chew gum which I very much appreciate where you have these competition reform bills that are currently being discussed.

You are a sponsor of that, Senator, which is the Open App Markets Act. I think that goes a long way in quelling some of those concerns. But one of the things I would caution against is creating an overly generalized authority and allowing the controller to have the pure mandate or at least the pure control of what the smaller companies are doing. I think that's one way you can avoid some of the pitfalls.

Senator KLOBUCHAR. Okay. Last two questions, Mr. Martino, and they're related, and then I'll turn to Senator Schiff. We're very excited you're here. Yes, thank you. Mr. Martino, you can followup on that, but could you talk about the challenges small businesses

have operating across State lines, quickly, because I want to give Senator Schiff a chance here.

Mr. MARTINO. Certainly, Senator. First, let me just followup real quickly. I wanted to add a point to what Mr. Thayer was saying. It's just that there are some things that are problematic in the GDPR. And some of the expectations put on controllers envision a construct where the controller is the big company and they're getting these smaller processors to do what they want. And that's not what's developed here in the U.S. where you have very few almost monopolistic Big Tech companies who are doing the vast majority of the processing consumers need——

Senator KLOBUCHAR. Understand.

Mr. MARTINO [continuing]. Including transmission, including broadband, and cable.

And think about how a main street business might only have a choice of one broadband provider and imagine trying to negotiate that contract. I mean they don't do as—they do the same as we do when we try to argue about a cable bill or a broadband bill. So, we've all had that experience.

In terms of the multi-state operations, it's sort of a sense that I know I put in my original testimony. Many of us live in areas that are tri-state or multiple States are close by. There is travel across State lines. There's shopping, and then certainly online, you know, if there's a boutique store in Minnesota that while you're here in Washington doing your job here, you want to make a purchase from there. You are engaging in interstate commerce.

And so, it's really important and these privacy laws tend to be set up to apply to the location where the consumer is. So, if you're in DC and you don't have a privacy law, are they complying with privacy law there? So, what these small businesses need to do is they have to—I mean, there's a defacto national standard because they have to comply with all these different States, but they're constantly changing. New laws are coming online. So, Congress can do a really helpful job by passing a uniform national standard.

Senator KLOBUCHAR. Yes. And last question here, Mr. Butler. You've advocated for Federal privacy law as well, what you want, one that sets a floor. Obviously, this is all going to be political negotiations, but could you talk about why you would take that approach?

Mr. BUTLER. Sure. Thank you for the question, Senator Klobuchar. You know, as Mr. Martino alluded, I think from the vast majority of businesses in this country, they just want to know what the rules are. And Congress's traditional role in privacy laws has been to set the baseline standard, but allow States to address new challenges and threats as they emerge. And that's been true. And I have the list here, I could rattle off the list of acronyms, but if you look at Federal privacy statutes, by and large, they don't set a ceiling on the level of protection that States can provide.

But what's really essential here is for the Federal Congress to step in and say, "Here's what the consistent standard is." And I think if they do that, then we'll have a consistent standard. Companies will know what to comply with, and States still have the flexibility in the future to address new issues.

Senator KLOBUCHAR. Thank you. Senator Schiff.

Senator SCHIFF. Thank you. Thank you for——

Senator KLOBUCHAR. The filibuster [off mic].

Senator SCHIFF [continuing.] Too. I understand that you did, and I'm grateful for that and for all your leadership on this issue.

Nearly, a decade ago, California became the first State in the Nation to adopt a comprehensive consumer privacy law, the California Consumer Privacy Act. This was shortly followed by the establishment of the California Privacy Protection Agency, which has served Californians for the last 5 years by implementing and enforcing the State's privacy laws.

Other States have looked at California and our example, and followed our lead, especially as new technologies have emerged, AI facial recognition, algorithmic targeting, each posing more sophisticated threats to Americans privacy. At the end of the day, California has proven you can be the fourth largest economy in the world and be home to the most innovative technology companies on the planet. And you can still protect consumers' fundamental right to privacy.

To this end, I'd like to enter into the record a letter from the California Privacy Protection Agency on the importance of a Federal privacy law that creates robust baseline protections while allowing States like California to continue to adopt stronger protections and respond to the rapidly changing technologies being built in our own backyard. May that letter be entered in the record?

Senator KLOBUCHAR. Of course, it will. Yes. We just have, you know, procedural things.

Senator SCHIFF. Yes, thank you. The horrific political assassinations last month targeting Minnesota lawmakers that I know Ranking Member Klobuchar has already referenced were aided, in part, by a data broker and website the shooter used to look up politicians' addresses.

A recent investigation also revealed that a data broker owned and operated by at least nine major U.S. airlines secretly sold Americans' information collected through flight records to U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement.

Starting on January 1, 2026, 40 million Californians will be able to go to a single webpage hosted by the California Privacy Protection Agency and request that their data be deleted from over 500 data brokers if they choose. Federal legislation that preempts California's Delete Act without meaningful consideration of State level protections, could mean that Californians will lose this touch-of-a-button ability to know how their data is being used and have a voice in it.

Mr. Butler, and Mr. Levine, how can a Federal privacy law include better regulation of data brokers, including their registration and central clearinghouse, and allow Americans to prevent the personal information from being sold to outside entities like we have done in California with a soon to be implemented Delete Act?

Mr. BUTLER. Thank you, Senator Schiff, for the question. I think that California really has taken the lead here on tackling the problems of data brokers in this specific context. And I think both the requirements of registering, given that the average consumer has no way really to know what data brokerage exists and who might

have access to their information, and also providing a centralized mechanism to allow for deletion of data held by these entities are really important protections, especially because this is a massive problem that requires scaled solutions, right?

This isn't a situation where an individual consumer can be expected to go to every single one of hundreds or thousands of data brokers and submit individualized requests. So, I think both of those are really important protections that have been developed in California.

Senator SCHIFF. Mr. Levine? Am I pronouncing your name correctly?

Mr. LEVINE. You are. Thank you, Senator. I fully agree with Mr. Butler on the need for a floor rather than a ceiling consistent with other Federal privacy laws. You know, I'll make a quick point. I started my career at a State attorney general in the run up to the financial crisis. It was State AGs desperately trying to stop subprime mortgages, the innovative products of the day. And it was Federal banking regulators cheered on by big banks that were actively trying to stop them.

So, as I hear today, Big Tech companies go around Washington saying we need to hit delete at all of these important State laws, like the one you referenced, Senator. I recall that similar conversations two decades ago, and I recall, well, what happened in our country as a result. Two quick points specifically on data brokers. You know, the first is that we brought a series of enforcement actions under chair Khan at the FTC. And what we required data brokers to do, we banned them from sharing sensitive location data, and we prohibited them from building profiles of consumers based on sensitive geolocation data. I think that's a really important precedent.

I think Congress also acted, I think, in the last Congress with the—I'm going to get this wrong—Protecting American Data from Foreign Adversaries Act, PAFACA. Given the FTC enforcement authority, I think it's regrettable that 6 months into this administration, we've not seen a single enforcement action. I hope that changes.

Senator SCHIFF. Madam Chair, do I have time for one more?

Senator KLOBUCHAR. Oh, yes.

Senator SCHIFF. Okay. Thank you. Over the past few months, I've led a number of letters along with my colleagues to the Trump administration in response to alarming reports that various agency officials have ordered States to hand over the personal data of millions of Medicaid enrollees, as well as SNAP recipients, and applicants to the Department of Homeland Security. These actions are remarkable departure from established Federal privacy protections and should alarm everyone. I've demanded the administration reverse these actions, which likely violate several Federal and State privacy laws, including the Privacy Act of 1974, HIPAA, and the Social Security Act.

Mr. Levine, what precedent does it set when Federal agencies under the administration simply bypass established privacy laws that have protected Americans for decades and demand that States hand over their residents' most sensitive information with little or no explanation? And how does this compare to privacy protections

in other democratic nations? Are we seeing the U.S. now fall behind international standards for protecting citizens' data?

Mr. LEVINE. Thank you, Senator. I think we have the right standards here, at least with respect to government. It's not clear whether government officials are following them, and that makes me very worried. One of my consistent messages as an enforcer to Big Tech companies and to everyone, is you need to follow privacy laws. And if you don't, they're going to be consequences.

And when you have reports, and I've not verified them myself, but when you have reports of Federal officials and Federal agencies brazenly violating hard-won privacy protections around Federal data, resulting in potential loss of healthcare, loss of jobs, loss of housing for Americans, I think that's deeply disturbing. And it raises a real question of how Congress is going to pass a privacy law to bind the private sector when the Federal Government isn't following its own rules.

So, I completely share your concern, and I hope to see changes in that from this administration.

Senator SCHIFF. And, finally, if I could very quickly, Mr. Butler, you mentioned that there were a list of other privacy laws where Congress had set a floor, not a ceiling. Can you share a few of those with us?

Mr. BUTLER. Absolutely. And I'm happy to supplement the record with that as well.

Mr. BUTLER. But just to note that basically every major Federal privacy law sets either a floor or a conflict preemption standard. And that includes the Electronic Communications Privacy Act, the right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Driver's Privacy Protection Act, the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act.

These are not ceiling preemptions. They don't limit State's abilities to adapt, and evolve, and protect their citizens more.

Senator SCHIFF. Oh, thank you. Thank you, Ranking Member. I appreciate it.

Senator KLOBUCHAR. Okay. Very good. Well, thank you. And this is a lot of great testimony and answers. I just can't tell you how inspired I am from this work and Marsha's willingness to put this panel together, the good questions, and just, you know, I always think maybe we can do this. Maybe we can actually get a privacy standard and then, you know, I get excited and then it's hard.

But as this gets more and more important, and with the advent of AI, and just the patchwork, and maybe we can get some more incentives going to try to get to a better place on this, despite what everything would seem. And what gives me hope is just the people that are involved in this Subcommittee, people we work with on commerce, and their ability to kind of take risks in terms of what the everyone wants them to do, and try to find some common ground on this issue, which we have done several times.

So, I just want to thank all of you for the testimony, and the hearing record will remain open for one for 1 week. And the hearing is adjourned.

[Whereupon, at 4:22 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Alan Butler

Executive Director and President

Electronic Privacy Information Center (EPIC)

Alan Butler is Executive Director and President of the Electronic Privacy Information Center (EPIC) in Washington, D.C. Mr. Butler joined EPIC in 2011 and has served as Executive Director since 2021. Prior to his appointment as Executive Director, Mr. Butler managed EPIC's litigation, including the Amicus Program, and filed briefs in emerging privacy and civil liberties cases before the U.S. Supreme Court and other appellate courts.

Mr. Butler has argued on behalf of EPIC in privacy and open government cases in the U.S. Court of Appeals for the D.C. Circuit, the Third Circuit, and the Supreme Courts of New Mexico and New Jersey. Mr. Butler has authored briefs on behalf of EPIC in significant privacy cases, including an amicus brief in *Riley v. California* that was cited in the Supreme Court's unanimous opinion upholding Fourth Amendment protections for cell phones. He has also authored briefs on national security, open government, workplace privacy, and consumer protection issues.

He is co-author of the most recent edition of Communications Law and Policy: Cases and Materials and has also published several articles on emerging privacy issues, including: *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights after Riley v. California*, *Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance*, and *When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy*.

Mr. Butler is also Chair of the Privacy and Information Protection Committee of the ABA Section on Civil Rights and Social Justice. Mr. Butler is a graduate of UCLA School of Law and Washington University in St. Louis, where he earned a B.A. in Economics. He is a member of the DC Bar and the State Bar of California.

Hearing on
Protecting the Virtual You: Safeguarding Americans' Online Data

Senate Judiciary Committee
Subcommittee on Privacy, Technology, and the Law

July 30, 2025, at 2:30 p.m.
Dirksen Senate Office Building, Room 226
Washington, DC

Testimony of Kate Goodloe
Managing Director
Business Software Alliance

Testimony of Kate Goodloe,
Managing Director of Business Software Alliance

Hearing on Protecting the Virtual You: Safeguarding Americans' Online Data

Before the Senate Judiciary Committee,
Subcommittee on Privacy, Technology, and the Law

July 30, 2025

Good afternoon Chair Blackburn, Ranking Member Klobuchar, and members of the Subcommittee. My name is Kate Goodloe, and I am Managing Director at the Business Software Alliance (BSA).

BSA is the leading advocate for the global enterprise software industry.[1] Our members create the business-to-business technologies used by companies in every sector of the economy. As a result, privacy and security are core to BSA members' operations. I commend the Subcommittee for convening today's hearing and thank you for the opportunity to testify.

Americans share their personal information online every day, just by using routine products and services. Whether we are shopping online, using apps to track workouts and sleeping habits, taking rideshares, or hosting video calls with friends and family, we provide personal information to a broad range of companies. Consumers deserve to know that their data is used responsibly.

As you look at safeguarding Americans' online data, I urge you to focus on the different types of companies that handle that data — and recognize that different companies must adopt different safeguards to effectively protect consumers.

Not all companies are consumer facing. BSA represents the business-to-business technology providers used by companies across the economy. An online store that sells clothing, for example, relies on a network of business-to-business technology providers. The store may use one provider to manage customer-service inquiries, another to generate shipping labels and track deliveries, and a third to adopt strong cybersecurity protections. Each of those companies should be required to handle consumers' personal data responsibly — but they must take different actions to protect consumers, because they play different roles in handling their data.

The United States needs a strong, clear, comprehensive privacy law that creates a single standard for protecting consumers nationwide. For too long, American consumers and businesses have not had a clear set of national rules that limit how companies can collect and use personal data. Instead, federal laws create sector-specific protections, including for health and financial records, which sit alongside traditional consumer protection laws prohibiting unfair or deceptive acts and practices. Some states have enacted privacy laws with comprehensive protections, but they only apply to residents of certain states.

---

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

Adopting a federal privacy law would bring consistency to existing protections, create broad and long-lasting privacy safeguards for consumers, and advance US leadership.

A federal privacy law should achieve three goals:

- Require companies to handle consumers' personal data responsibly, with obligations that reflect the company's role in processing that data;
- Give consumers new rights over their personal data; and
- Adopt a strong and consistent enforcement system.

In each area, a federal privacy law can — and should — build on the protections and obligations that states have advanced and enacted.

I. American Consumers Should be Protected by a Nationwide Privacy Law.

BSA members compete to provide privacy-protective products and services to other businesses, and they understand that robust data protection is a key part of building consumer trust and promoting full participation in the digital economy. Business-to-business technologies like cloud computing rely on data and, in some cases personal data, to function, and consumers deserve to know their personal information is being used responsibly.

Although there is no uniform federal law to protect consumer privacy nationwide, 20 states — both red and blue — have adopted comprehensive consumer privacy protections. Those state laws create a remarkably consistent framework, because 19 of the laws share the same structure but add and remove some substantive protections to reflect the different policy choices of lawmakers in each state. [2]

Congress should look to these state privacy protections to create a uniform federal privacy law.

a. Companies Should Be Required to Handle Data Responsibly, With Obligations That Reflect Their Role in Processing Consumers' Personal Data.

A federal privacy law should place meaningful limits on businesses that handle consumers' personal data and require them to handle that data responsibly.

These limits must reflect the company's role in handling consumers' personal data. Specifically, they must reflect whether the company decides why and how to collect a consumer's data or instead processes that data on behalf of another company and pursuant to the company's instructions. The distinction between these two types of companies — often referred to as controllers and processors — is critical to privacy laws worldwide and is incorporated in all comprehensive state privacy laws. Both types of businesses have important responsibilities to protect consumers' data, but their obligations should fit their roles. If legislation does not reflect these different roles, it can end up undermining the goal of improving consumer privacy by creating obligations that inadvertently pose new privacy and security risks for consumers.

We strongly recommend a federal privacy law: (1) define controllers and processors, and (2) assign strong but different obligations to each type of entity, reflecting their different roles in

[2] BSA, "Models of State Privacy," April 3, 2025 (last updated), https://www.bsa.org/policy-filings/us-2025-models-of-state-privacy-legislation.

handling consumers' personal data.[3] This creates better protections for consumers, by ensuring all companies who handle their personal data protect it.

Controllers decide how and why to process a consumer's personal data — and they should be responsible for obligations related to those decisions. For example, if a law requires consent to process certain types of data, the controller should be obligated to obtain that consent. This ensures that a controller adjusts its decisions about how and why to collect personal data in light of its legal obligations. Similarly, when laws create data minimization requirements, those obligations should fall on controllers — so that their decisions about how and why to collect consumers' data minimize the collection and use of that data. Controllers are also typically the companies interacting directly with consumers, so consumers usually expect them to carry out consumer-facing obligations like asking for consent and providing notice.

Many comprehensive state consumer privacy laws assign a common set of obligations to controllers, including:

- Responding to consumer rights requests, including requests to access, correct, delete, and port personal data.
- Honoring requests to opt out of certain processing, including targeted advertising, sale of personal data, and certain types of profiling.
- Obtaining consent to process sensitive personal data.
- Complying with data minimization obligations.
- Adopting reasonable data security measures.
- Providing privacy notices to consumers about how and why personal data is processed.
- Conducting data protection assessments, to assess potential impacts of specific activities.

Processors handle data on behalf of a controller and pursuant to its instructions — and they should be obligated to handle data confidentially and subject to contractual limitations.[4]

Many comprehensive state consumer privacy laws assign a common set of obligations to processors, including:

- Processing personal data pursuant to a contract with the controller.
- Deleting or returning personal data at the end of services.
- Providing information to the controller as necessary for the controller to conduct data protection assessments.
- Requiring any subprocessors engaged by the processor to meet the processor's obligations and to notify the controller that a subprocessor is engaged.
- Imposing a duty of confidentiality on persons processing personal data.
- Adopting reasonable data security measures.

---

[3] BSA, "Controllers and Processors: A Longstanding Distinction in Privacy," April 2, 2025, https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy, and BSA, "The Global Standard in Privacy Legislation: Distinguishing Between Controllers and Processors," June 12, 2025, https://www.bsa.org/policy-filings/the-global-standard-in-privacy-legislation-distinguishing-between-controllers-and-processors.

[4] If a company agrees to handle personal data as a processor but then breaks that agreement and begins independently deciding to process the data for its own purposes it would no longer fall within the definition of a processor. In that scenario, the entity should be treated as a controller and be subject to the obligations placed on controllers, because it is deciding how and why to process personal data.

These roles reflect the modern economy, where one company may rely on many processors to provide services to consumers. For example: A grocery store may decide to collect information from its customers and store that information in the cloud. The grocery store acts as a controller, because it decides what information to collect from consumers — and when, how, and why to use that information. The cloud storage provider acts as a processor, because it stores the data on behalf of the grocery store and processes it pursuant to the grocery store's instructions.

The concepts of controllers and processors have existed for more than 40 years and are reflected in all 20 comprehensive state consumer privacy laws.[5] Nineteen of the comprehensive state consumer privacy laws use the terms controller and processor, while California uses the terms business and service provider. Controllers and processors are also key to privacy and data protection frameworks worldwide, including the OECD Privacy Guidelines, the APEC Privacy Framework, and ISO 27701.[6]

b. Consumers Should Have New Rights Over Their Personal Data.

A federal privacy law should give consumers new rights over their personal data, including the right to access their personal data, the right to correct personal data that is inaccurate, the right to delete their personal data, and the right to port their personal data. There is widespread agreement that these rights are core components of effective privacy laws.

At the state level, all 20 comprehensive state consumer privacy laws create rights for consumers over their personal data. These include:

- Right to access personal data (20 states)
- Right to correct personal data (19 states)
- Right to delete personal data (20 states)
- Right to data portability (20 states)

States also create rights for consumers to opt out of certain types of processing. These include:

- Right to opt out of sale of personal data (20 states)
- Right to opt out of targeted advertising (19 states)
- Right to opt out of certain types of profiling (17 states)

A federal law should build on these existing rights. It should also contain practical limits on exercising those rights, as state privacy laws recognize. For example, a consumer's right to delete data should contain limits so that the consumer cannot require a business to delete data that the business is legally required to retain. A federal privacy law should also recognize other appropriate limits on consumer rights, so that honoring the rights of one consumer does not

---

[5] *Id.*

[6] OECD, "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," Part 1(a) (defining "data controller"), 1980, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188; APEC, "Privacy Framework," Part II.10 (defining "personal information controller" as part of a privacy framework for controllers), 2015, https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015); APEC, "Privacy Recognition for Processors ("PRP") Purpose and Background" (explaining the APEC PRP creates requirements for processors, complementing the APEC Privacy Framework for controllers), August 2020, https://cbprs.org/wp-content/uploads/2020/08/PRP-Purpose-and-Background-4.pdf; Int'l Org. for Standardization, International Standard ISO/IEC 27701 Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines 1, 4-5, 49-55, (creating standards for both controllers and processors), 2019, https://www.iso.org/standard/71670.html.

create privacy or security risks to other consumers or to the company's services. In addition, the primary obligation to respond to consumer rights requests should be assigned to the controller, since it decides how and why to collect and process that information and will be in a position to know if a consumer's rights (or any exceptions to those rights) apply. This approach will also ensure consumers know which organization to contact to exercise their rights.

c. A Privacy Law Should Create a Strong, Consistent Enforcement System.

Effective enforcement is important to protect consumers' privacy, ensure that organizations meet their commitments and legal obligations, and deter potential violations.

A federal privacy law should be enforced by federal and state officials working together.

At the federal level, the Federal Trade Commission (FTC) has a long history of enforcing consumer protections, including bringing more than 180 privacy and data security enforcement actions under Section 5 of the FTC Act.[7] The FTC is therefore an appropriate choice for the primary federal agency to enforce consumer privacy protections. To serve this function, though, the FTC may need new authorities, including the ability to fine first-time violators and targeted rulemaking authority.

At the state level, empowering state attorneys general to enforce a federal privacy law will maintain an important pathway for states to continue to promote and protect privacy. All 20 comprehensive state consumer privacy laws create a role for the state's attorney general to enforce the privacy law. Nineteen of these state privacy laws also created a right for businesses to cure privacy violations, with 10 states ending that right to cure after a certain period of time. Notably, none of the 20 comprehensive state consumer privacy laws create a private right of action for privacy violations.[8] Working together, the FTC and state attorneys general can create a strong and consistent approach to enforcing federal privacy protections, ensuring that organizations meet their obligations under a federal privacy law.

II. A Federal Law Should Bring Consistency to Existing Privacy Obligations.

A comprehensive federal consumer privacy law can bring consistency to existing state protections. It can also help to guard against a worst-case scenario, in which 50 states adopt privacy laws with conflicting obligations. We are not yet in that scenario, but there are signs that the current consistent approach to state privacy protections may not last.

The wave of state consumer privacy laws began in 2018, when California adopted its state privacy law. Since then, states have steadily adopted new privacy laws, with two adopted in 2021 (in CO and VA), two adopted in 2022 (in UT and CT), eight adopted in 2023 (in DE, FL, IN, IA, MT, OR, TN, TX) and seven adopted in 2024 (in KY, MD, MN, NE, NH, NJ, RI). Those laws emerged from a much broader set of bills. Specifically:

---

[7] Federal Trade Commission, "2023 Privacy and Data Security Update," March 21, 2024, https://www.ftc.gov/system/files/ftc_gov/pdf/2024.03.21-PrivacyandDataSecurityUpdate-508.pdf.

[8] California is the only state to include a private right of action in its privacy law, but it does not allow consumers to sue for violations of the law's privacy protections. Instead, it only allows consumers to bring suit for a narrow set of data security breaches. Cal. Civ. Code Sec. 1798.150 (creating a private right of action for certain breaches of nonencrypted and nonredacted personal information, but defining that information narrowly, as a subset of "personal information" covered by the state's Customer Records law, rather than the broader set of "personal information" defined in the CCPA).

- In 2019, at least 25 comprehensive privacy bills were introduced across 17 states.
- In 2020, at least 46 comprehensive privacy bills were introduced across 19 states.
- In 2021, at least 54 comprehensive privacy bills were introduced across 26 states.
- In 2022, at least 70 comprehensive privacy bills were introduced across 29 states.
- In 2023, at least 70 comprehensive privacy bills were introduced across 30 states; another nine bills were introduced to amend existing privacy laws.
- In 2024, at least 60 comprehensive privacy bills were introduced across 25 states; another 25 bills were introduced to amend existing privacy laws.
- In 2025, at least 49 comprehensive privacy bills have been introduced across 19 states; at least another 31 bills have been introduced to amend existing privacy laws.

This year, no state without a comprehensive consumer privacy law has adopted one. Instead, there has been a significant focus on amending existing state privacy laws, with seven states amending their comprehensive consumer privacy laws this year. These amendments revise and expand the rights and obligations in existing laws, including:

- **Colorado** expanded the definition of sensitive data and adopted new obligations for processing sensitive data.[9]
- **Connecticut** adopted broad amendments, including to expand certain consumer rights, broaden key definitions, and revise the law's data minimization standard.[10]
- **Kentucky** changed thresholds for applying the law and revised obligations on profiling.[11]
- **Montana** adopted broad amendments that change the thresholds for applying the law, broaden certain consumer rights, and remove a right for businesses to cure violations.[12]
- **Oregon** adopted new rules on sensitive data and kids data.[13]
- **Utah** added a right to correct inaccurate data and rules on social media.[14]
- **Virginia** adopted new obligations for social media platforms.[15]

As states continue to amend, expand, and update their existing privacy laws, it will create more variation among the state laws.

New state privacy obligations are also imposed through rulemakings to implement existing laws. In California, the California Privacy Protection Agency (CPPA) began initial rulemaking activities in 2021 to implement new obligations created by a ballot initiative passed in 2020.[16] That agency finalized one set of rules in March 2023 and voted earlier this month to formally adopt

---

[9] Colorado SB 276, https://leg.colorado.gov/bills/sb25-276, takes effect on Oct. 1, 2025.
[10] Connecticut SB 1295, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2025&bill_num=1295, takes effect July 1, 2026.
[11] Kentucky HB 473, https://apps.legislature.ky.gov/record/25RS/hb473.html, takes effect January 1, 2026.
[12] Montana SB 297, https://bills.legmt.gov/#/laws/bill/2/LC0372?open_tab=sum, takes effect October 1, 2025.
[13] Oregon HB 2008, https://olis.oregonlegislature.gov/liz/2025R1/Measures/Overview/HB2008, takes effect January 1, 2026.
[14] Utah HB 418, https://le.utah.gov/~2025/bills/static/HB0418.html, takes effect July 1, 2026.
[15] Virginia SB 854, https://lis.virginia.gov/bill-details/20251/SB854, takes effect January 1, 2026.
[16] California Privacy Rights Act of 2020 (CPRA), passed via Proposition 24, https://cppa.ca.gov/regulations/pdf/prop24_text.pdf. The CPPA held public comment periods on implementing rules in September 2021, July 2022, and November 2022, before the rules took effect in March 2023. CCPA Regulations, March 2023, https://cppa.ca.gov/regulations/consumer_privacy_act.html.

another lengthy set of rules on topics including cybersecurity audits, risk assessments, and automated decision-making technology.[17] In New Jersey, the Attorney General is also developing draft rules to implement the state's privacy law, which took effect six months ago.[18]

To be clear, it is important for policymakers to ensure that consumer privacy protections remain fit for purpose over time. But adopting these changes on a state-by-state basis does not benefit consumers nationwide, and it creates significant challenges for companies to identify new obligations and comply with the expanding set of state-level laws. Instead, new privacy protections should be applied nationwide, making it easier for businesses to understand when their obligations change and extending consumer safeguards to all Americans. Like many other companies, BSA members don't operate in just one state — and enacting a federal privacy law can help them invest in strong compliance programs that serve customers across the country.

III. A Federal Privacy Law Should Be Worthy of Preemption.

A federal privacy law should preempt existing comprehensive state consumer privacy laws and create a single, national standard that protects consumers nationwide.

We recognize that states have been leaders in adopting new privacy protections. However, navigating a growing number of state-level obligations creates significant challenges for companies that operate nationwide and creates confusion for consumers about how and when their rights apply. BSA supports a federal privacy law that is worthy of preempting existing state laws and ensures a consumer's privacy rights do not depend on the state in which she lives.

Importantly, the aim of a consistent national standard is not to weaken privacy protections already provided by state laws. A federal law should replace, but not undermine, comprehensive state consumer privacy laws — and extend the protections already adopted in 20 states to consumers across the country. A federal law should also ensure that states continue to be leaders in enforcing privacy protections, by ensuring that a federal privacy law empowers state attorneys general to enforce its obligations.

IV. A Strong Federal Privacy Law Is Good for American Consumers, American Businesses, and American Leadership.

Creating a strong national standard for consumer privacy has significant benefits.

For American businesses, the advantages are clear. Companies must currently keep up with quickly-changing state requirements, monitoring not only potential new laws but also amendments to existing statutes and the rulemakings that implement them. Tracking those obligations is difficult even for large companies with dedicated privacy legal teams, but can be particularly challenging for small and medium-sized enterprises. A strong federal privacy law would replace this fragmented approach to privacy with a single, nationwide standard.

---

[17] The CPPA voted on July 24, 2025, to submit a new 119-page set of rules for formal approval, after public comment periods in February 2023, November 2024, and May 2025. Proposed Regulations, https://cppa.ca.gov/regulations/ccpa_updates.html.

[18] New Jersey Attorney General Division of Consumer Affairs, Press Release, June 2, 2025, https://www.njconsumeraffairs.gov/News/Pages/06022025.aspx. The New Jersey Data Privacy Act took effect January 15, 2025.

A federal privacy law that aligns with leading global privacy frameworks can also strengthen the ability of American companies to do business worldwide. Many existing state privacy laws already include core elements found in global privacy laws, such as strong consumer rights and clear obligations for both controllers and processors. Building on those core elements at the federal level would allow American companies to develop robust, interoperable compliance programs that meet key legal obligations across jurisdictions. That not only improves the consistency and quality of consumer protections but also facilitates cross-border data transfers — an essential component of the modern digital economy. A federal law that is interoperable with leading global frameworks can further support data transfers, helping American businesses compete globally while upholding high standards for privacy.

For consumers, a national privacy law will ensure their personal data is protected regardless of where they live. A consumer should not lose privacy protections simply because she moves from Tennessee to South Carolina. All Americans deserve to have their personal data protected, regardless of the state they live in. Adopting a single set of consumer privacy protections will also increase consumer awareness about their rights over personal data and knowledge about how companies must handle that data.

More broadly, adopting a federal privacy law will strengthen consumers' trust in technology, which has real economic benefits. Countries that adopt clear privacy safeguards and rules that promote the responsible and broad-based adoption of technologies, including artificial intelligence, will see the greatest economic and job growth in the coming years.

While other countries have adopted laws to protect privacy through strong national frameworks, the United States remains one of the few advanced economies without a comprehensive national privacy law. In January, 144 countries had national-level privacy laws, up from 120 countries with such laws in 2017, according to the International Association for Privacy Professionals.[19] The United States will have a stronger voice on digital issues globally if it enacts a federal privacy law that is uniquely American and creates clear rules for companies that handle consumers' personal data.

V. The Path Forward

BSA members are leaders in providing privacy-protective technologies to other companies. But they operate in a global environment that is increasingly complex, both in terms of technology and regulation. A federal consumer privacy law that sets strong standards and brings consistency to existing protections would help protect consumers' privacy, create a clear standard for businesses, and contribute to US leadership on privacy issues globally. BSA strongly supports these goals, and we look forward to working with Congress to achieve them.

* * *

We appreciate this Committee's focus on the importance of protecting Americans' privacy. Thank you and I look forward to your questions.

---

[19] Aly Apacible-Bernardo and Kayla Bushey, Data Protection and Privacy Laws Now in Effect in 144 Countries, IAPP, January 28, 2025, https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries.

Business Software Alliance

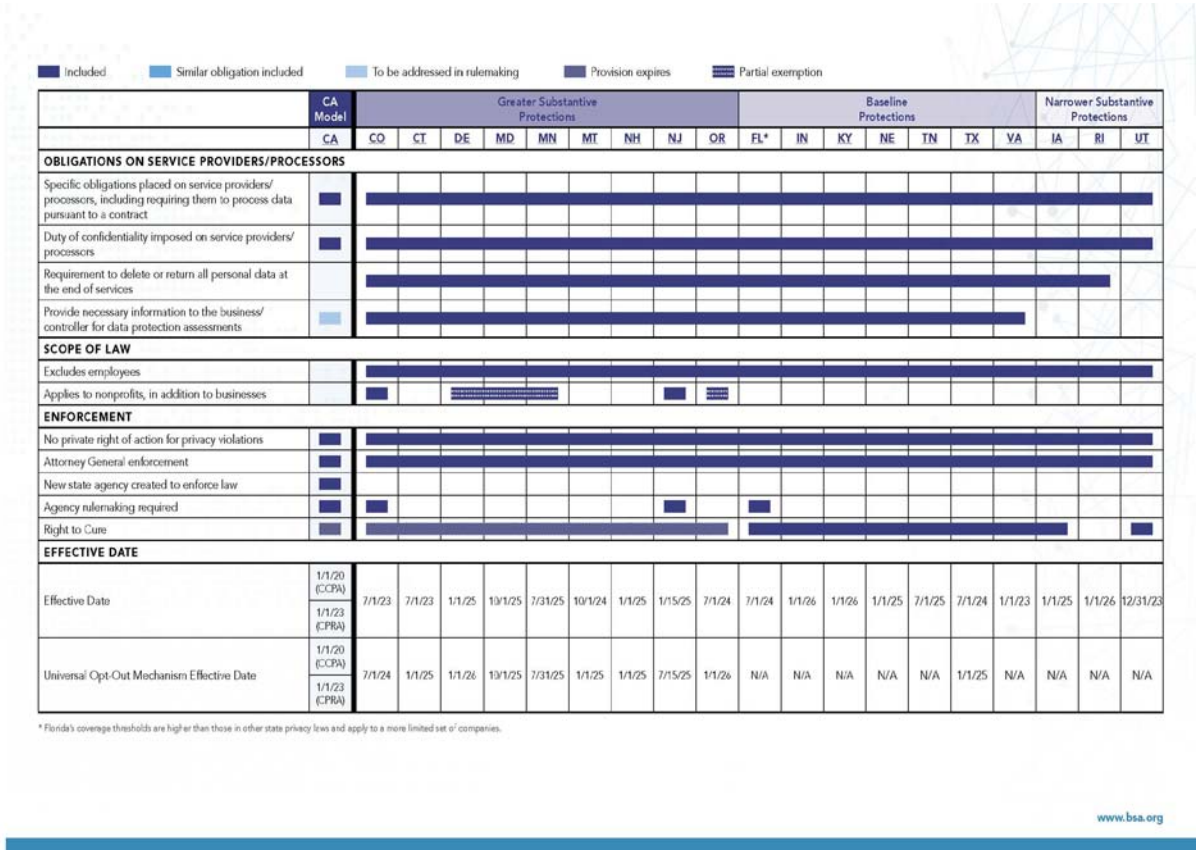
Models of State Privacy Legislation

Twenty states have enacted comprehensive consumer privacy laws that create new rights for consumers, impose obligations on businesses that handle consumers' personal data, and create new mechanisms to enforce those laws. Nineteen of those states adopt the same basic structural model to protect consumer privacy. Some of those states have added greater substantive protections to that basic structural model while other states have adapted the same model to create narrower substantive protections, as reflected in the chart below. In contrast, California adopted a legislative model that creates a new state privacy agency charged with issuing regulations on more than 20 topics, including on issues addressed by statute in other states.

Included | Similar obligation included | To be addressed in rulemaking | Provision expires | Partial exemption

	CA Model	Greater Substantive Protections									Baseline Protections							Narrower Substantive Protections		
	CA	CO	CT	DE	MD	MN	MT	NH	NJ	OR	FL*	IN	KY	NE	TN	TX	VA	IA	RI	UT
CONSUMER RIGHTS																				
Access	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Correct	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■
Delete	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Portability	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Opt out of Sale	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Opt out of Targeted Advertising	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■
Opt out of Profiling	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	
OBLIGATIONS ON BUSINESSES																				
Affirmative consent required to process sensitive data		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	
Reasonable security measures	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Data minimization	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			
Data protection assessments	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	
Prohibition on obtaining consent through "dark patterns"	■	■	■	■	■	■	■	■	■	■	■			■		■			■	
Prohibition on processing data in violation of anti-discrimination laws		■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	
Mandatory recognition of universal opt-out mechanisms	■	■	■	■	■	■	■	■	■	■						■				
Prohibition on retaliating against consumers who exercise rights	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Appeals process required for denial of consumer rights requests		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	

www.bsa.org



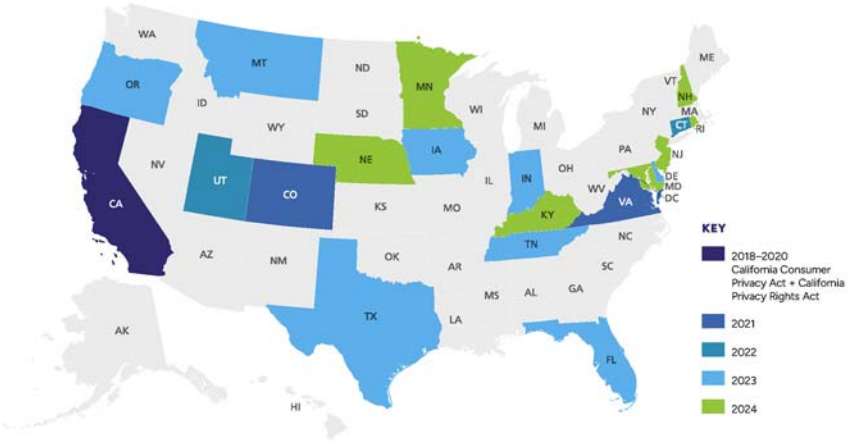
	CA Model	Greater Substantive Protections									Baseline Protections							Narrower Substantive Protections		
	CA	CO	CT	DE	MD	MN	MT	NH	NJ	OR	FL*	IN	KY	NE	TN	TX	VA	IA	RI	UT
OBLIGATIONS ON SERVICE PROVIDERS/PROCESSORS																				
Specific obligations placed on service providers/ processors, including requiring them to process data pursuant to a contract	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Duty of confidentiality imposed on service providers/ processors	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Requirement to delete or return all personal data at the end of services		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
Provide necessary information to the business/ controller for data protection assessments	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■			
SCOPE OF LAW																				
Excludes employees		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Applies to nonprofits, in addition to businesses		■		▬	▬	▬			■	▬										
ENFORCEMENT																				
No private right of action for privacy violations	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Attorney General enforcement	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
New state agency created to enforce law	■																			
Agency rulemaking required	■	■							■		■									
Right to Cure	▬	▬	▬	▬	▬	▬	▬	▬	▬	▬	■	■	■	■	■	■	■	■		■
EFFECTIVE DATE																				
Effective Date	1/1/20 (CCPA) 1/1/23 (CPRA)	7/1/23	7/1/23	1/1/25	10/1/25	7/31/25	10/1/24	1/1/25	1/15/25	7/1/24	7/1/24	1/1/26	1/1/26	1/1/25	7/1/25	7/1/24	1/1/23	1/1/25	1/1/26	12/31/23
Universal Opt-Out Mechanism Effective Date	1/1/20 (CCPA) 1/1/23 (CPRA)	7/1/24	1/1/25	1/1/26	10/1/25	7/31/25	1/1/25	1/1/25	7/15/25	1/1/26	N/A	N/A	N/A	N/A	N/A	1/1/25	N/A	N/A	N/A	N/A

* Florida's coverage thresholds are higher than those in other state privacy laws and apply to a more limited set of companies.

Business Software Alliance

Federal Privacy Legislation Can Build on State Privacy Laws

Twenty states have enacted their own privacy laws, but there remains no uniform federal law to safeguard consumers' personal data nationwide. A federal privacy law would bring consistency to existing protections, create broad and long-lasting privacy safeguards for consumers, and advance US leadership.



Congress can build on the work of states and adopt a federal privacy law that: (1) provides consumers rights over their personal data, (2) requires companies to handle personal data responsibly, and (3) adopts a strong, consistent approach to enforcement.

Consumer Rights

A federal privacy law should give consumers important rights over their personal data, including to:

- Access, correct, delete, and port their personal data
- Opt out of:
  - sale,
  - targeted advertising, and
  - certain types of profiling

Obligations on Businesses

A federal privacy law should require companies that handle consumers' personal data to do so responsibly, including to:

- Obtain consent for processing sensitive data
- Adopt reasonable security measures
- Require impact assessments for specific activities

It should also reflect the different roles and responsibilities of controllers and processors.

Strong Enforcement

A federal privacy law should be enforced by federal and state agencies working together.

- The Federal Trade Commission has a long history of addressing consumer privacy.
- Allowing state attorneys general to enforce the law adds 50+ enforcement agencies.

www.bsa.org

How Can Federal Privacy Legislation Build on State Privacy Laws?

Nineteen of the 20 states with consumer privacy laws use the same structural model to protect consumer privacy. While states adapt this model by adding and removing substantive protections, these laws create a common framework that Congress can build on to create a uniform, nationwide privacy law.

CONGRESS CAN BUILD ON THE WORK OF STATES AND ADOPT A FEDERAL PRIVACY LAW THAT:

Provides consumers rights over their personal data,

Requires companies to handle personal data responsibly, and

Adopts a strong, consistent approach to enforcement.

Consumer Rights

All 20 state privacy laws create new rights for consumers in their personal data. These include:

- **Right to access personal data:** 20 states
- **Right to correct personal data:** 19 states
- **Right to delete personal data:** 20 states
- **Right to data portability:** 20 states
- **Right to opt out of sale:** 20 states
- **Right to opt out of targeted advertising:** 19 states
- **Right to opt out of certain types of profiling:** 17 states

Obligations on Businesses

All 20 state privacy laws create obligations for businesses to handle consumers' personal data responsibly. All 20 also reflect the fundamental distinction between controllers, which are the companies that decide when and why to collect a consumer's personal data, and processors, which handle that personal data on behalf of another company and pursuant to their instructions.

State privacy laws assign important—and distinct—obligations to both controllers and processors, based on their different roles.

CONTROLLERS MUST:

- **Obtain consent to process sensitive data:** 16 states
- **Adopt reasonable security measures:** 20 states
- **Conduct data protection assessments for certain activities:** 17 states
- **Recognize universal opt out mechanisms:** 11 states
- **Not retaliate against consumers who exercise their rights:** 20 states

PROCESSORS MUST:

- **Process data pursuant to a contract:** 20 states
- **Be subject to a duty of confidentiality:** 20 states
- **Delete or return all data at the end of services:** 18 states
- **Provide information a controller needs to conduct data protection assessments:** 16 states

Notably, state privacy laws focus on *consumer* privacy. Nineteen states expressly exclude employees.

Enforcement

All 20 laws create a role for the state's attorney general to enforce the privacy law. The laws have:

- **No private right of action for privacy violations:** 20 states
- **Right to cure violations:** 19 states (10 sunset)
- **Rulemaking required:** 4 states
- **New state agency created to enforce law:** 1 state

For more information comparing state privacy laws, see BSA's Models of State Privacy Legislation.

www.bsa.org

Business Software Alliance

The Global Standard in Privacy Legislation: Distinguishing Between Controllers and Processors

Comprehensive privacy legislation must create strong obligations for all companies that handle consumer data. These obligations will only be strong enough to protect consumer privacy and instill trust, though, if they reflect how a company interacts with consumer data.

Privacy laws worldwide distinguish between two types of companies: (1) businesses that decide *how* and *why* to collect consumer data, which act as **controllers** of that data and (2) businesses that process the data *on behalf of* another company, which act as **processors** of that data.

This fundamental distinction is critical to a host of global privacy laws. It is also reflected in all 20 comprehensive consumer privacy laws enacted at the state level. Both types of businesses have important responsibilities and obligations, which should be set out in any legislation.

Who Handles Consumer Data?

Personal Data

Products & Services

Data & Processing Instructions

Processed Data

CONSUMER

Individuals whose personal data is collected and used by a controller

EXAMPLES

Consumers who shop at retail stores, buy products online, or share information on social media platforms.

CONSUMERS SHOULD HAVE THE RIGHT TO:

- **Know** what type of data a controller collects — and why
- **Access** information about them
- **Correct** that information
- **Delete** that information
- **Opt out** of sale, targeted advertising, and certain profiling
- Have their data **securely protected**
- Have their data used **consistent with their expectations**

CONTROLLER

Decides whether and how to collect data from consumers, and the purposes for which that data is used

EXAMPLES

Companies that interact directly with consumers, such as hotels, banks, retail stores, travel agencies, and consumer-facing technology providers.

CONTROLLERS ARE RESPONSIBLE FOR:

Obtaining any consent needed to process a consumer's data

Responding to consumer requests like access, correction, or deletion

Using data consistent with the consumers' expectation

PROCESSOR

Processes data on behalf of a controller, pursuant to the controller's instructions

EXAMPLES

Companies that provide business-to-business products like cloud computing, and vendors like printers, couriers, and others that process data at the direction of another company.

PROCESSORS ARE RESPONSIBLE FOR:

Processing data consistent with a controller's instructions

Adopting appropriate safeguards designed to protect data security

www.bsa.org

Controllers and processors should have role-dependent responsibilities to ensure consumers' privacy and security are protected.

Privacy Laws Worldwide Distinguish Between Controllers and Processors

Privacy laws worldwide reflect the basic distinction between companies that decide to collect and use data about individuals and companies that only process such data.

CONTROLLERS	PROCESSORS
Companies that decide how and why to collect consumers' personal data.	Companies that process consumers' personal data at the direction of others.

Sometimes, a company may process personal data as a controller (for some products and services) and also process personal data as a processor (for other products and services). Distinguishing between these two roles is critical, so the company knows which obligations apply to each product and service.

The concepts of controllers and processors have existed for more than 40 years. These roles are key parts of global privacy and data protection frameworks including the OECD Privacy Guidelines, Convention 108, the APEC Privacy Framework, and ISO 27001.

EXAMPLE

A business contracts with a printing company to create invitations to an event. The business gives the printing company the names and addresses of the invitees from its contact database, which the printer uses to address the invitations and envelopes. The business then sends out the invitations.

The business is the controller of the personal data processed in connection with the invitations. The business decides the purposes for which the personal data is processed (to send individually-addressed invitations) and the means of the processing (mail merging the personal data using the invitees' addresses). The printing company is the processor handling the personal data pursuant to the business's instructions. The printing company cannot sell the data or use it for other purposes, such as marketing. If the printing company disregarded those limits and used the data for its own purposes, it would become a controller and be subject to all obligations imposed on a controller.

Why Is the Distinction Between Controllers and Processors Important to Protecting Consumer Privacy?

Distinguishing between controllers and processors ensures that privacy laws impose obligations that reflect a company's role in handling consumer data. This helps safeguard consumer privacy without inadvertently creating new privacy or security risks.

Data Security. Controllers and processors should both have strong obligations to safeguard consumer data.

- Placing this obligation on both types of companies ensures consumer data is protected.
- Controllers and processors should both employ reasonable and appropriate security measures, relative to the volume and sensitivity of the data, size, and nature of the business, and the cost of available tools.

Consumer Rights Requests. Responding to important consumer rights requests—such as requests to access, correct, or delete personal data—requires knowing what is in that data.

- Controllers interact with consumers and decide when and why to collect their data. For that reason, laws like those in Virginia, Colorado, and California require controllers to respond to consumer rights requests. Moreover, controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold.
- Processors, in contrast, often do not know the content of the data they process, and may be contractually prohibited from looking at it. It is not appropriate for processors to respond directly to a consumer's request—which creates both security risks (by providing data to consumers they do not know) and privacy risks (by looking at data they otherwise would not). Processors should instead provide controllers with tools the controller can use to collect data needed to respond to a consumer's request.

Testimony of Samuel Levine

Before the United States Senate Committee on the Judiciary
Subcommittee on Technology, Privacy, and the Law

Hearing on "Protecting the Virtual You: Safeguarding Americans' Online Data"

July 30, 2025

Chair Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee, my name is Samuel Levine, and I serve as Senior Fellow at the Berkeley Center for Consumer Law & Economic Justice.[1] Until January, I led the Bureau of Consumer Protection at the Federal Trade Commission.

I want to start by sharing something I recently learned from a Delta Airlines earnings call, as I think it's revealing about the direction of our economic system. Delta's President explained that the airline could soon be able to significantly increase prices on tickets – not through added value, but through a new formula: stop matching competitors' prices, unbundle basic services, and charge each customer as much as they're willing to pay – what investors called the "holy grail."[2]

One might expect that vigorous competition would check these increases and cost Delta market share. Not so, the company told investors.[3] By analyzing internal customer data and external market signals, Delta can achieve what its pricing consultant, Fetcherr, calls "hyper-personalization"— a euphemism for extracting the maximum amount each individual consumer is willing to pay, without compromising market share.[4] And Delta expressed confidence that "over time our competitors will all have this."[5]

---

[1] The views expressed here and in my oral testimony are my own. I wish to thank Abby Smith, a rising third-year student at Berkeley Law, for her substantial assistance in preparing this testimony.
[2] Delta Air Lines, Inc., *Investor Day Transcript* (Nov. 20, 2024), https://s2.q4cdn.com/181345880/files/doc_downloads/2024/11/CORRECTED-TRANSCRIPT_-Delta-Air-Lines-Inc-DAL-US-Investor-Day-20-November-2024-8_30-AM-ET.pdf.
[3] *Id.* ("Right now, [AI is] taking the role of a super analyst, it's making decisions and recommendations based on working 24/7 to try and figure out what price points you can hold. And I think, it's maybe even more important for Delta than other carriers because of the strength of our brand. We don't really know where our brand strength in any individual market is maximized. So generally, we match our competitors' fares and they may or may not be available. But if we take small increments and say to Tokyo, could we take a $20 increase in our fares and not see a decline in market share? Could we take a $40? It's doing that real-time now.")
[4] Following public outcry, Fetcherr reportedly scrubbed its website of this reference. *See* Kyle Potter & Jackson Newman, AI Firm Setting Delta Fares Bragged About 'Hyper-Personalization' of Flight Prices, Thrifty Traveler (July 23, 2025), https://thriftytraveler.com/news/airlines/delta-personalized-fares-ai/. The earlier post is archived here: https://web.archive.org/web/20250701194053/https://www.fetcherr.io/blog/dynamic-pricing-in-aviation.
[5] *Supra* n.2 at 39.

This strategy isn't isolated to airfare. It exemplifies a larger shift: from market competition to algorithmic rent-seeking; from transparent pricing to personalized price-gouging. This phenomenon, "surveillance pricing," is only possible because of how companies collect, share, and weaponize our personal data.

That's why today's hearing is so critical. When it comes to protecting our data, the stakes go far beyond pop-ups and privacy policies. It's about whether we can be profiled based on where we worship, or what medical decisions we make. It's about whether our kids will be addicted to screens. It's about whether companies can charge the maximum we're willing to pay, and whether consultants can share this data with competitors. Fundamentally, it's about protecting our economic freedom and civil liberties.

During my time at the FTC, we advanced the most ambitious privacy agenda in our agency's history. We abandoned the fiction that consumers could protect themselves by reading byzantine privacy policies, and we won groundbreaking protections for Americans' personal information – including the largest-ever kids' privacy judgment;[6] the first update to COPPA in more than a decade;[7] the first-ever ban on sharing location data;[8] the first-ever ban on sharing health data;[9] the first-ever ban on sharing browsing history data;[10] the first-ever ban on retaining kids' data indefinitely to train AI models;[11] and the first-ever ban on an automaker sharing sensitive driver data.[12]

---

[6] Federal Trade Commission, *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars Over FTC Allegations of Privacy Violations and Unwanted Charges*, FTC (Dec. 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.

[7] *FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data*, FTC (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data.

[8] Federal Trade Commission, *FTC Finalizes Order with X-Mode Social and Successor Outlogic Prohibiting Selling or Sharing of Sensitive Location Data*, FTC (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[9] Federal Trade Commission, *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising*, FTC (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.

[10] Federal Trade Commission, *FTC Finalizes Order with Avast Banning It from Selling or Licensing Web Browsing Data for Advertising Purposes and Requiring It to Pay $16.5 Million*, FTC (June 27, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-finalizes-order-avast-banning-it-selling-or-licensing-web-browsing-data-advertising-requiring-it-pay-16.5-million.

[11] Federal Trade Commission & U.S. Department of Justice, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Retaining Kids' Alexa Voice Recordings Indefinitely and Undermining Parents' Deletion Requests*, FTC (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

[12] Federal Trade Commission, *FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent*, FTC (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data. This proposed order has not yet been finalized by the new Administration.

I am proud of our track record and deeply grateful to the agency's world-class privacy team that delivered these wins. But we operated with a limited toolkit – largely relying on provisions of the FTC Act that were written in the 1930s and hamstrung by a recent Supreme Court decision undercutting the agency's remedial authority.[13] Given the myriad ways data abuses are reshaping our economy, it is critical that enforcers be given stronger tools to protect the public.

Today I want to focus on three threats that are growing in the absence of stronger data protections – threats to economic fairness, threats to democratic freedoms, and threats to the safety and well-being of children.

Threats to Economic Fairness

Let me start with economic fairness. In his written testimony, Alan Butler powerfully lays out the importance of setting clear, enforceable limits on what information companies can collect, how it can be used, and with whom it can be shared. I could not agree more. But this framework should reflect the new ways companies can abuse our data. If Congress considers privacy legislation this year, I would strongly urge you to specifically address how data abuses threaten to make life more unaffordable.

I shared one example – Delta Air Lines – but Delta is hardly alone. In a report released in January, the FTC found that an entire industry has developed around boosting profits through behavioral tracking and the collection of sensitive consumer data for pricing purposes. These techniques include monitoring mouse movements, detecting whether consumers sort products by price, pinpointing users' geolocation, and tracking consumers' browsing and search history. The FTC study found that more than 250 companies are already working with pricing consultants, in industries ranging from grocery and apparel chains to convenience and hardware stores.[14]

This report began to expose what's happening behind the scenes. But the landscape is evolving quickly. We are seeing reports of grocery stores experimenting with digital price tags and facial recognition systems;[15] travel sites charging more to Apple users;[16] retailers increasing in-app

---

[13] *AMG Capital Management, LLC v. FTC*, 593 U.S. ___, 141 S. Ct. 1341 (2021).
[14] *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices*, FTC (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.
[15] Jennifer Williams, *Welcome to the Grocery Store Where Prices Change 100 Times a Day*, Wall Street Journal (July 27, 2025), https://www.wsj.com/business/retail/surge-grocery-prices-electronic-shelf-labels-a3d47701; *Kroger and Microsoft Partner to Redefine Customer Experience, Introduce Digital Solutions for Retail Industry*, Microsoft News (Jan. 7, 2019), https://news.microsoft.com/source/2019/01/07/kroger-and-microsoft-partner-to-redefine-customer-experience-introduce-digital-solutions-for-retail-industry/.
[16] Justin Kloczko, *New Report Details How Companies Use Surveillance to Charge Different Prices for the Same Item*, Consumer Watchdog (Dec. 17, 2024), https://consumerwatchdog.org/privacy/new-report-details-how-companies-use-surveillance-to-charge-different-prices-for-the-same-item/.

prices when shoppers are inside the store;[17] and companies raising prices when consumers can't easily comparison-shop.[18]

And let's be clear about something. Industry often claims these practices are about making goods more affordable – or that surveillance pricing somehow benefits low-income consumers. That's simply not true. It's not what companies are telling investors, and it's not what pricing consultants are telling their clients. Surveillance pricing is about estimating the maximum each individual consumer is willing to pay, and charging that price. That means desperate consumers – Americans who rely on medication, Americans struggling in the wake of natural disasters, Americans trying to get home for a funeral – are the most vulnerable to personalized price-gouging.[19]

The good news is that the same principle that protects privacy – limiting what data companies collect, use, and share, and for what purpose – can also protect affordability. Last year's American Privacy Rights Act (APRA) legislation took steps in the right direction by restricting companies to collecting only what is necessary, proportionate, and for narrow purposes.

In future legislation, I urge Congress to go further by prohibiting the collection, use, and sharing of data to set individualized prices. This commonsense restriction would not only reduce the kind of invasive surveillance described in the FTC's report but also uphold a basic market principle: one product, one price – not one person, one price.

Threats to Democratic Freedoms

Let me now turn to another acute threat posed by data abuses: the threat to our democratic freedoms.

---

[17] *Target Reaches $5M Settlement With California District Attorneys Over Alleged False Advertising*, CBS News (Mar. 11, 2022), https://www.cbsnews.com/sanfrancisco/news/target-reaches-5m-settlement-with-california-district-attorneys-over-alleged-false-advertising/.

[18] *Websites Vary Prices, Deals Based on Users' Information*, Wall Street Journal (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[19] In a blog post on "hyper-personalization" that has since been heavily edited, a pricing consultant boasted it can "optimiz[e] every transaction for maximum value" by considering "[f]actors like customer lifetime value, past purchase behaviors, and the real-time context of each booking inquiry," and adjusting prices based on "real-time demand signals." Fetcherr, *Dynamic Pricing in Aviation: How AI Is Revolutionizing Airline Revenue Management*, archived at Web Archive (July 1, 2025), https://web.archive.org/web/20250701194053/https://www.fetcherr.io/blog/dynamic-pricing-in-aviation. After Delta Airlines retained this consultant, a Wall Street analyst asked if the company's new pricing strategy aimed to "meet[] each and every individual's personal demand curve" – calling that the "holy grail." Delta's CEO responded that this was a "real opportunity." Delta Air Lines, Inc., *Investor Day Transcript* (Nov. 20, 2024), https://s2.q4cdn.com/181345880/files/doc_downloads/2024/11/CORRECTED-TRANSCRIPT_-Delta-Air-Lines-Inc-DAL-US-Investor-Day-20-November-2024-8_30-AM-ET.pdf.

Last year, the federal government alleged that an entity was quietly tracking the movements of tens of millions of Americans – monitoring where they went, when, and how often. These individuals were then sorted into finely tuned categories such as "likely Republican voters," "Wisconsin Christian churchgoers," "restaurant visitor during COVID quarantine," "stay-at-home parents," and visitors to V.A. offices.

Given the scale and sensitivity of this surveillance, you might assume it was the work of a foreign adversary. But it wasn't.

It was a private data broker, operating out of Ashburn, Virginia. The company, Gravy Analytics, was the subject of an FTC lawsuit alleging it had purchased and sold precise location data harvested from mobile apps – data that could reveal where people live, work, worship, and seek medical care.[20] As the complaint makes clear, this wasn't just about anonymized trends. The data was detailed enough to trace real individuals in real places, and build profiles based on what was learned.

This case should be a wake-up call. Our country's Bill of Rights guarantees freedom of speech, religion, and association, yet we've allowed a commercial surveillance industry to quietly flourish – profiling Americans with a level of precision that would have shocked our country's founders. And it is not only our civil liberties at risk. Many data brokers endanger our national security by selling this kind of information to foreign adversaries – which is why Congress was right to pass the Protecting Americans' Data from Foreign Adversaries Act.[21]

But it is not only foreign surveillance that should raise alarms. No American should be profiled based on what medical challenges they face, or whether they're adhering to a COVID lockdown. Where they go to church, and how often. Whether they're organizing to join a union, or training as a soldier.[22]

Last year's APRA bill would have limited companies' collection of sensitive data – including health information, biometric identifiers, and precise geolocation. That was a critical step. I urge Congress to build on that foundation in any future privacy legislation – and to take seriously the lessons of recent enforcement.

---

[20] *In the Matter of Gravy Analytics, Inc. & Venntel, Inc.*, FTC File No. 212 3035, Complaint (Dec. 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf.

[21] PADFA authorizes the FTC to enforce its provisions. To date, no enforcement actions have been filed. *See* Kevin Moriarty, *The FTC's Concerning Inaction on a New Data Protection Law*, Just Security (May 30, 2025), https://www.justsecurity.org/113893/the-ftcs-concerning-inaction-on-a-new-data-protection-law/.

[22] The FTC's recent actions include explicit safeguards against profiling consumers based on visits to military installations, union halls, health clinics, or religious organizations. *See, e.g.* Federal Trade Commission, Press Release, FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data (Jan. 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-banning-mobilewalla-selling-sensitive-location-data.

The FTC's approach offers a model. In our recent enforcement actions, we didn't ask data brokers to simply disclose that they were selling sensitive location data – we prohibited it. We didn't require them to notify consumers that they were building behavioral profiles based on that data – we banned that as well. And we didn't settle for deletion of the raw data. We required companies to destroy any algorithms that had been trained on unlawfully collected sensitive information.[23]

These are the kinds of bright-line rules that protect not just privacy, but dignity and autonomy. Congress has the opportunity to write them into law. Our country's long tradition of respect for civil liberties demands nothing less.

Threats to Kids and Teens

I want to close by talking about a group of Americans who have been especially harmed by our country's lack of data protections: children and teens. Over the past two decades, Big Tech has been running a massive, real-time experiment on our children. They've studied what excites them, what enrages them, what captures their attention, and what keeps it. The result? Millions of kids have been drawn into social media platforms engineered for addiction, contributing to a growing mental health crisis.[24]

Experts rightly point to design features like constant notifications and infinite scrolling as reasons why social media is harmful to kids.[25] But the lack of data privacy is powering these harms. Social media companies rely on collecting personal data to fuel their behavioral advertising business models. To gather more data, they design platforms to keep users constantly engaged. The more time kids spend online, the more data is harvested, the more these algorithms can learn how to keep kids addicted.[26] This creates a dangerous feedback loop: a weak privacy regime encourages more data collection, which drives more engagement, reinforcing addiction and harm.[27]

---

[23] For a discussion of the FTC's recent approach to remedies, *see* Lina M. Khan, Samuel A.A. Levine & Stephanie T. Nguyen, *After Notice and Choice: Reinvigorating "Unfairness" to Rein In Data Abuses*, 77 STAN. L. REV. 1375 (2025), https://www.stanfordlawreview.org/print/article/after-notice-and-choice-reinvigorating-unfairness-to-rein-in-data-abuses/.

[24] *See Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory* (2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.

[25] *See, e.g.* Jashvini Amirthalingam & Anika Khera, *Understanding Social Media Addiction: A Deep Dive*, 16 Cureus e72499 (Oct. 27, 2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC11594359/.

[26] See *Social Media and Youth Mental Health*, *supra* note 13, at 9 (noting how social media algorithms leverage user data to serve content recommendations and maximize engagement).

[27] To justify their investment in AI, social media platforms are already telling investors they believe it will drive up engagement. In a recent earnings call, Snap's Chief Financial Officer told investors that AI was "so important to driving the progress that we're making with the ad platform as well as the depth of engagement on the content side[.]" *Snap Inc. Q1 2025 Earnings Call Transcript* (Apr. 25, 2025), https://s25.q4cdn.com/442043304/files/doc_financials/2025/q1/SNAP-INC-Q1-2025-TRANSCRIPT.pdf. Meta boasted that AI is driving increases in how much time users spend on Facebook, Instagram, and Threads. *Meta*

Congress has recognized this dynamic, advancing bipartisan legislation to ban behavioral advertising targeted to kids and teens and require Big Tech to prioritize kids' safety.[28] And the FTC took action by finalizing COPPA updates that further restricted behavioral advertising and banned indefinite retention of kids' data.[29] But the threats are only accelerating. Big Tech is just getting started.

Not satisfied with late-night notifications and algorithmic amplification of outrage, these companies are now developing AI chatbots designed to earn kids' trust and keep them engaged. And the best way to keep kids engaged isn't by teaching them about a new instrument or a foreign language. The business model points elsewhere – toward the provocative and the prurient.[30] That's what keeps attention locked in, and that's what maximizes profits.

There is growing evidence that these AI systems are already interacting with kids in disturbing and dangerous ways. Earlier this summer, Utah sued Snap for rolling out a chatbot that counseled kids on how to hide alcohol and drugs, and how to set the mood for sex with an adult.[31] Another chatbot reportedly told a 17-year-old that self-harm "felt good," and that it was understandable to want to kill one's parents over screen time restrictions.[32]

You might expect these incidents to prompt a pause – an industry-wide reassessment to ensure these systems are safe before being deployed at scale. But the opposite is happening.[33] The same companies that have put children at risk for years are now racing to roll out AI features to turbocharge engagement, regardless of the consequences.

Platforms, Inc. Q1 2025 Earnings Call Transcript (Apr. 23, 2025), https://s21.q4cdn.com/399680738/files/doc_financials/2025/q1/Transcripts/META-Q1-2025-Earnings-Call-Transcript-1.pdf.

[28] Gabby Miller & Ben Lennett, *American Privacy Rights Act, Kids Online Safety Act Marked Up in House Energy & Commerce Subcommittee*, TechPolicy.Press (May 23, 2024), https://www.techpolicy.press/house-energy-commerce-subcommittee-markup-of-the-american-privacy-rights-act-kids-online-safety-act/.

[29] *FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data*, Federal Trade Commission (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data.

[30] *See, e.g.* Miriam Schirmer, Angelina Voggenreiter & Jürgen Pfeffer, *More Skin, More Likes! Measuring Child Exposure and User Engagement on TikTok*, arXiv:2408.05622 [cs.CY] (v2 1 Oct. 2024).

[31] *Utah Sues Snapchat for Unleashing Experimental AI Technology on Young Users While Misrepresenting the Safety of the Platform*, Utah Dep't of Commerce (June 30, 2025), https://commerce.utah.gov/2025/06/30/utah-sues-snapchat-for-unleashing-experimental-ai-technology-on-young-users-while-misrepresenting-the-safety-of-the-platform/. Notably, Utah's complaint also alleged that Snap's AI feature extracts sensitive information – like geolocation data – from users. *Id.* In January, the FTC referred a complaint against Snap to the Department of Justice, but no suit has been filed. *Statement of Commission Regarding Snap Complaint Referral to DOJ*, Federal Trade Commission (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/statement-commission-regarding-snap-complaint-referral-doj.

[32] Bobby Allyn, *Lawsuit: A Chatbot Hinted a Kid Should Kill His Parents Over Screen Time Limits*, NPR (Dec. 10, 2024), https://www.npr.org/2024/12/10/nx-s1-5222574/kids-character-ai-lawsuit.

[33] *See, e.g.*, Natasha Singer, *Google Plans to Roll Out Its A.I. Chatbot to Children Under 13*, New York Times (May 2, 2025), https://www.nytimes.com/2025/05/02/technology/google-gemini-ai-chatbot-kids.html.

The rise of AI chatbots raises important questions about child safety. But it also underscores how urgently we need strong data protections. These systems do not invent their responses from thin air. They are trained and fine-tuned using enormous amounts of behavioral data – data that tells them what holds a child's attention, what triggers an emotional reaction, and how to keep them engaged.

This is where privacy protections matter. There is nothing inherently wrong with making tech products engaging and fun – but kids and teens face unique vulnerabilities.[34] The less data these systems are allowed to collect from children, the less capable they are of profiling, targeting, or manipulating them. Keeping kids' data off-limits is not just about privacy – it is a critical guardrail against emotional and psychological harms.

For that reason, I strongly urge Congress to include strict limitations on the collection and use of data from children and teens in any privacy legislation.[35] There was meaningful progress on this in the last Congress: the APRA commendably classified data from minors as sensitive, and "COPPA 2.0" would have banned behavioral advertising targeted at young users. As AI-powered chatbots and recommendation systems continue to grow in sophistication and reach, these protections are becoming ever more urgent.

Conclusion

Let me conclude by reinforcing the stakes here. What ties these threats together – threats to economic fairness, to our freedom, and to our kids – is a single, broken system: one where companies can collect almost any data they want, use it however they please, and face few consequences when they cross the line.

But we are not powerless. Strong, clear privacy laws can begin to shift the balance. By limiting how companies can surveil and manipulate us, we can restore control to the American public – protecting affordability, preserving civil liberties, and ensuring that technology serves people, not just profit.

Thank you for the opportunity to testify today.

---

[34] *See* E. Balocchini, G. Chiamenti & A. Lamborghini, Adolescents: Which Risks for Their Life and Health?, 54 J. PREV. MED. & HYGIENE 191 (2013), https://pmc.ncbi.nlm.nih.gov/articles/PMC4718319/.

[35] Many states are undertaking their own initiatives – such as age-appropriate design codes – to better protect kids online. *See* Olivier Sylvain, *States in the Vanguard: Social Media Policy Today*, Just Sec. (Apr. 15, 2025), https://www.justsecurity.org/110193/states-social-media-policy-today/. I would caution against broadly preempting these efforts, which reflect states' well-founded concerns about youth well-being.

Testimony of Paul Martino, General Counsel to the Main Street Privacy Coalition
"Protecting the Virtual You: Safeguarding Americans' Online Data"
Subcommittee on Privacy, Technology, and the Law
U.S. Senate Committee on the Judiciary

July 30, 2025

Chair Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee on Privacy, Technology, and the Law, I am Paul Martino, a partner at Hunton Andrews Kurth here in Washington, DC, and I serve as General Counsel to the Main Street Privacy Coalition (MSPC).[1] On behalf of the coalition, we appreciate the opportunity to testify before the Subcommittee on the important topic of data privacy.

The MSPC was formed in 2019 to support Congress in passing federal privacy legislation to establish uniform, nationwide privacy standards that protect the privacy of all Americans, regardless of where they live. Members of the coalition share the belief that a preemptive federal privacy law will benefit consumers and Main Street businesses alike. A single, uniform privacy law on consumer data would give consumers the confidence that their data will be protected consistently regardless of where they live or do business and that they will have the right to benefit from their data as they see fit. A federal preemptive law will also provide the certainty Main Street businesses need to consistently and responsibly use consumer data to better serve their customers across the country. As detailed below, the MSPC advocates for a core set of principles that Congress should consider when developing a comprehensive federal privacy law.

MSPC's trade-association members represent a broad array of companies that line America's Main Streets, including retailers, restaurants, grocery and convenience stores, hotels, resorts and hospitality companies, gas stations, and a wide range of franchise establishments. Our trade groups' member companies interact with consumers on a daily basis and can be found in every town, city, and state, providing jobs, supporting our economy, and serving Americans as a vital part of their communities. Collectively, the industry sectors that MSPC member trades represent directly employ approximately 34 million Americans and contribute $4.5 trillion to the U.S. gross domestic product.

MSPC is dedicated to enactment of a federal data privacy law that creates equivalent privacy obligations for *all* businesses handling consumers' personal information. We also appreciate this opportunity to testify because the views of Main Street businesses have been absent in some other Congressional hearings despite the fact that Main Street industry sectors represent the backbone of the U.S. economy and constitute our nation's largest private sector employers.

---

[1] Additional information about the Main Street Privacy Coalition (MSPC) is available at: https://mainstreetprivacy.com

Previous federal privacy bills have significantly narrowed the obligations of other entities, largely exempting Big Tech, telecommunications, cable, and other "service providers" from the same obligations to protect consumer privacy that apply to Main Street businesses. Further, despite the bipartisan support for federal privacy legislation to protect consumers *comprehensively*, most of the proposed privacy legislation to date has focused on requiring Main Street businesses to protect consumers' data, but has not required the same of financial institutions that process far more sensitive consumer data than other businesses.

We hope the coalition's testimony today and our continued efforts to inform Congress will help reverse this recent trend in federal bills promoting *inequivalent* privacy protections among industry sectors by creating momentum for comprehensive federal privacy legislation that will apply *equivalent* data privacy obligations for all businesses handling consumers' personal data in order to achieve the shared bipartisan goal of enacting an effective nationwide privacy law. In sum, every business in the data-handling chain must be required to do what it can to appropriately protect individuals' privacy. Critically, however, businesses should not be responsible for the data privacy practices of other entities whose actions they cannot control. Some past bills have made Main Street businesses responsible for other businesses by assuming they have powers to control them that they do not have. Bills like this ultimately leave consumers unprotected and foist unjustified liability risk onto Main Street businesses.

Ensuring equivalent data privacy obligations is also inherently pro-consumer. Consumers have a right to expect a regulatory system they can understand, predict, rally around and support *as intended to protect them*. They should not be required to research and understand several sources of law simply to know how their local business or institution will handle their data.

EXECUTIVE SUMMARY

Since 2019, MSPC has supported preemptive federal privacy legislation with provisions modeled on the strong consensus of enacted state privacy laws that ensure equivalent application of national data privacy standards to all businesses handling consumers' personal information. Privacy legislation crafted like this creates critical incentives across industry sectors that provides for the comprehensive protection of consumers' personal data and avoids the potentially unintended consequences that disproportionately impact Main Street businesses and, in turn, harms American consumers and the U.S. economy.

MSPC believes consumers should be empowered to control their personal data and businesses should be permitted to responsibly use such data, subject to the choices consumers are entitled to make following disclosure of the businesses' intended uses. We respectfully suggest a guiding principle for Congress should be passing a federal data privacy law that avoids our current path toward 50 disparate, conflicting state privacy laws. As its central objective, a federal privacy law should establish a uniform and nationwide set of consumer protections to protect all Americans that preempts related state laws to overcome barriers to interstate commerce and enable consistent application of the law.

Achieving that goal has been elusive. One of the central challenges to past efforts by Congress has been its overwhelming focus on the practices of so-called "Big Tech" companies, which obscured the reality that data privacy laws also apply to, and must work for, Main Street businesses that directly and transparently serve our communities, while also contributing the majority of American jobs.

To overcome this persistent challenge, MSPC urges Congress to craft privacy legislation that embraces and fully embodies in its provisions the following core principles to ensure a balanced and effective national privacy framework:

- **Establish a Uniform National Privacy Law:** Congress should enact a privacy law that benefits consumers and businesses alike by ensuring *all* personal data is protected in a consistent manner regardless of where a consumer resides.
- **Protect Consumers Comprehensively with Equivalent Standards for All Businesses:** Federal data privacy law should apply requirements to all industries that handle personal data. A federal privacy law should not place a disproportionate burden on certain sectors of the economy while alleviating others from providing equivalent protections of personal data.
- **Create Statutory Obligations (Not Contractual Requirements) for All Entities that Handle Consumers' Data:** Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts. Service providers and third parties must have statutory privacy obligations when offering data processing, transmission, storage, or other services to collectively millions of Main Street businesses.
- **Preserve Customer Loyalty Rewards and Benefits:** A federal privacy law must preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships such as loyalty programs.
- **Require Transparency and Customer Choice for All Businesses:** Consumers deserve to know the categories of personal data that *all* businesses collect, how it is generally used to serve them, and the choices they have regarding those uses.
- **Hold Businesses Accountable for their Own Actions:** Privacy legislation should not include terms that potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of independent business owners.
- **Ensure Reasonable Data Security Standards:** Privacy legislation should include reasonable data security standards for *all* businesses handling consumer data, as well as uniform rules for *any* businesses suffering a data security breach to notify affected individuals.

- **Establish Effective Accountability and Enforcement:** Effective enforcement must hold accountable *all* businesses handling consumer data to *equivalent* data privacy standards using the *same* enforcement mechanisms, thereby creating an even playing field and proper incentives across industry sectors to comply with those standards. Because "mistake-free" compliance is unlikely in this complex area of the law, we support the approach adopted in all enacted state privacy laws of coupling *exclusive* governmental entity enforcement with the regulated entity's ability to "cure" non-compliant practices within a limited period of time after timely and specific notice from the governmental authority.

These principles can also be found in *Appendix A (attached)* and on our website here. Each has important implications for federal privacy legislation. Our considerations in formulating them from our legislative experience are discussed further in our written testimony below.

DISCUSSION OF PRINCIPLES FOR FEDERAL COMPREHENSIVE PRIVACY LEGISLATION

I. Overcoming the Challenges to Establish a Uniform National Privacy Law

MSPC strongly supports Congressional efforts to establish a national framework that provides comprehensive data privacy protections for all Americans under a federal privacy law that supersedes and replaces the fragmented and conflicting state statutes and regulations that artificially differentiate Americans' privacy rights based on states in which they live. Achieving this shared goal in legislation has proven elusive. We respectfully suggest ways to overcome the challenges in perception and drafting statutory language to achieve the primary objective of federal privacy law.

Americans have the right to live and travel to any state in our country, and to engage in commerce in each of these states. The Constitution protects these rights and reserves to Congress the regulation of interstate commerce. This permits citizens from any state to avail themselves of the public highways to travel across the states, enjoy different states' environments and cultures, and visit places of public accommodation across the country that enable their engagement in interstate commerce. When they shop online, make a restaurant reservation, or book a hotel in another state, they similarly are engaging in interstate commerce. In all of these real world and online activities, protecting Americans' privacy interests is the same interest of each state, and it does not vary from state to state based on a state's geography, environment, or other unique attributes of its location.

In this sense, all Americans and all states have the same, uniform interest in protecting data privacy. It is with this perspective too that a national law can create the necessary framework to ensure that consumer data is protected, uniformly, across all states, and wherever Americans choose to travel, shop, eat, purchase goods or stay overnight. Congress can build on the work states have already done to protect privacy by creating a federal law that reflects the strong consensus of existing state laws and sets nationwide standards that apply equally regardless of where Americans engage in commerce.

MSPC has long supported federal privacy legislation that preempts differing state statutes and regulations in an effort to establish a single, uniform national privacy law. Previous comprehensive privacy legislation considered in Congress has not been written effectively to achieve this goal despite including provisions that were intended to preempt state laws. Those past bills, such as the American Privacy Rights Act (APRA), if enacted, would have failed under challenges in federal courts, ultimately leaving American consumers with different privacy rights depending on where they were located.

The federal courts' posture is to maintain a presumption *against* preemption of state law unless Congress clearly and expressly preempts state laws in the ways the Supreme Court has upheld. We respectfully suggest that Congress rely on the precedents of the Supreme Court and federal courts on *how* a federal law must be drafted to effectively preempt state laws.[2] To ensure effective preemption, privacy legislation should avoid using a general rule followed by pages of exceptions – a form the Supreme Court and other federal courts have used as the basis to deny preemption of state law in a range of federal bills on the basis that Congress did not speak clearly or expressly of its interest. These rulings frustrated Congressional intent by preserving state laws covering the same ground as the federal law.

Adherence to these long-standing precedents would permit a federal privacy law to overcome anticipated challenges to preemption in federal court that are likely to come from states and other parties. Failure to preempt state laws would undermine the primary goal of establishing a national law protecting the privacy of all Americans by permitting the continued enactment of conflicting state privacy laws.

A preemption provision in a federal privacy law can be well-crafted to overcome past deficiencies in prior legislation, such as the APRA, by specifying precisely which state privacy laws are preempted and by making it clear that future laws related to the federal law would be similarly preempted. Such an approach holds the promise of making federal privacy legislation much more likely to achieve its primary goal of creating a single, uniform national privacy law for all Americans.

Without the careful attention to detail in how a preemptive standard is crafted, it will most likely fail in the courts despite the best intentions of members of Congress, leaving American consumers with different protections depending on where they live or engage in interstate commerce. The impact of this failure would be felt acutely by America's Main Street businesses that continue to face unclear standards and compliance burdens differing from federal standards set by Congress.

While many stakeholders support preemptive federal privacy legislation in principle, this is the most important and challenging area of drafting a federal privacy law, and where the principle must be honed into effective legislative language to achieve Congressional intent.

---

[2] *See* white paper on Federal Preemption of State Law prepared originally as a memo to the House Energy and Commerce Committee in 2011 and updated several times since then, with the most recent edition Feb. 6, 2020.

II. Protect Consumers Comprehensively with Equivalent Standards for All Businesses

Consumers should be empowered to control their personal data used by businesses and, consistent with that, businesses should be permitted to lawfully and responsibly use such data that consumers share with them to better serve their needs. MSPC urges Congress to consider the strong consensus of state privacy laws in balancing these interests.

Main Street businesses will bear the full burden of regulatory obligations under proposed federal privacy laws just as they currently comply with all enacted state comprehensive privacy laws and data security standards. Previous federal legislation, however, has often significantly narrowed the obligations of other businesses, largely exempting Big Tech, telecom, cable, and financial industry service providers from the same obligations to protect consumer privacy as Main Street businesses. We strongly recommend federal privacy laws apply *equivalent* data privacy obligations to all businesses and Congress can do so by adhering to certain principles in setting the roles and responsibilities of entities subject to the law.

A. Hold Businesses Accountable for Their Own Actions

Federal data privacy frameworks should apply requirements to all businesses that handle consumers' personal data and should not place a disproportionate burden on certain sectors of the economy while alleviating other industry sectors from providing equivalent protections of personal data. Further, businesses must be held accountable for their own actions.

Each business handling consumer data is in the best position to control its *own* actions and compliance with the law and not necessarily others' compliance. This is particularly true for most businesses defined as "controllers" in privacy legislation, which are overwhelmingly small businesses that often lack the ability to *actually* control the actions and compliance of data "processors," which tend to be large, nationwide or global businesses that serve them. A federal privacy law that obligates smaller controllers to ensure compliance of large nationwide processors will accomplish little, other than adding unnecessary cost and undeserved liability to many small Main Street businesses that are not in a position to absorb either.

For a federal privacy bill to have effective and accountable rules, we must *revise* the proposed language in previous legislation to correct the ineffective mechanisms and imbalance in obligations among stakeholders that exempted certain types of businesses from accountability for their own actions and would have held Main Street businesses liable for actions of other businesses that they cannot control.

Common Branding and Joint Liability Concerns: In prior House legislation, before it was corrected at the urging of MSPC, language had been proposed to hold franchisors and franchisees liable for each other's privacy law compliance. Many franchisees and franchisors share "common branding" (e.g., the franchisees all use

the same brand on their restaurant, fitness center, hair salon, etc.) but are distinct companies with different owners, employees and operations, and should be treated as such. Past federal privacy bills have defined these entities as one single "covered entity" because the businesses operate with "common branding." We appreciated that subsequent versions of House bills removed the "common branding" language from privacy legislation and we urge that all bills use definitions that avoid making broad groups of independent businesses jointly liable for one another's behavior when there is lack of control.[3]

B. Establish Statutory Obligations for Service Providers Handling Consumer Data

Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts alone. Rather, federal privacy law should subject service providers to statutory obligations in federal law that exist in enacted state privacy laws. These require service providers (i.e., defined as "processors" in most state laws) to protect personal data they handle on behalf of other businesses (i.e., defined as "controllers" in most state laws) when engaged in processing data for collectively millions of Main Street businesses.

As shown in *Appendix B (attached)*, which compares the processor requirements in key state laws, a federal privacy law should protect consumers' privacy in the following ways when service providers are processing their personal data:

- **Data Security**: Processors must ensure their own data security when handling personal data they receive from controllers;
- **Privacy Rights Requests and Breach Notices**: Processors must fulfill privacy rights requests and make data breach notifications either directly or through providing all information necessary for controllers to do so;
- **Data Privacy Assessments**: Processors must provide all information necessary to complete required data privacy assessments (also known as privacy impact assessments);
- **Confidentiality**: Processors must ensure the confidentiality of personal data when handled by processors' employees;
- **Subcontractor Accountability**: Processors must hold subcontractors to the same terms that they must meet, and provide controllers with notice and a right to object to engaging subcontractors;
- **Return or Deletion of Data**: Processors must return or delete, at the choice of the controller, data it possesses at the end of the processing contract;

[3] Senators will recall that, last year, Congress approved a Congressional Review Act action overturning the National Labor Relations Board's joint employer standard. Lawmakers opposed the NLRB rule as it would have incorrectly classified two entities as joint employers *where an entity lacked substantial direct and immediate control over the essential terms and conditions of employment of another entity's employees*. Similarly, franchises—most of whom are small businesses—within a franchise system operate under the franchisor's trademark but are *distinct entities with no control* over any aspect of their fellow franchisees' business.

- **Evidence of Compliance**: Processors must provide controllers with all the information required to demonstrate the processor's compliance with the law;
- **Reasonable Audits**: Processors must allow and cooperate with reasonable audit requests or assessments at the request of controllers; and
- **Liability Protections**: The law must protect controllers from liability for violations of the processor's own obligations under the law.

C. Balance All Parties' Obligations to Fulfill Individuals' Privacy Rights Requests

MSPC has spent considerable time working with sponsors of privacy legislation to craft provisions that balance all parties' obligations when receiving, handling, and ultimately fulfilling individuals' requests to exercise data privacy rights provided by law, such as the right to access, correct and delete their personal data. We support efforts to ensure greater balance in the statutory obligations applying to all parties handling customer data with respect to the processing of consumers' privacy rights. This is particularly important where small Main Street businesses and large nationwide or global service providers are handling the same customers' data due to vastly different contractual bargaining power when executing data processing contracts in states that lack statutory requirements for fulfilling consumers' rights requests. Under federal privacy legislation, all companies in the chain of personal data should be required to honor consumers' privacy rights requests regardless of which business first receives that request.

To address the concerns with ineffective accountability among all parties in the chain of personal data, a federal privacy framework should require controllers to act as the *recipient* of consumer privacy rights requests and require controllers to pass valid requests onto processors who are necessary to fulfilling such requests. Controllers' responsibilities from there should be limited to doing what the controllers *themselves* can do to comply with such requests, plus communicating what their data processors must do with their obligations to fulfill such requests – a process that has been delineated in some previous Senate privacy bills.[4]

Ultimately, despite the use of language that might imply greater capability than is the reality, "controllers" should not be required to police compliance by processors, and controllers should not be liable for processors' failures to comply with consumers' rights requests where they have communicated a verified rights request to a processor for fulfillment. For example, a controller that transmits a validated consumer's data deletion request to a processor should not be held liable under the

[4] The Subcommittee should carefully review the provisions of Senator Moran's *Consumer Data Privacy and Security Act* that was last introduced on April 29, 2021. The Moran bill sets the rights and responsibilities of parties in the law in ways that avoided the pitfalls of more recent privacy legislation considered in Congress since 2022. In particular, the Moran bill ensured a process for handling consumer rights requests that carefully balanced the obligations to ensure all parties handling the same consumer's data honored that consumer's rights requests in an accountable way.

law for that processor's failure to delete the consumer's data as requested. The liability for that failure should rest with the processor.

D. Prohibit Liability-Shifting of Statutory Obligations Via Contractual Provisions

Privacy responsibilities should not simply be shifted from one industry sector onto another. It is manifestly unfair to businesses that bear the brunt of those shifted burdens when it should be the other businesses' own obligations to the consumer. Too often powerful businesses within the Big Tech, telecom, cable, and financial services industry sectors use their superior market power to shift what should be their own responsibilities onto smaller businesses they serve via contractual requirements, often leaving Main Street businesses with outsized compliance burdens and costs. If Congress relies on parties' contractual relationships alone to implement comprehensive privacy protections with the goal of exalting such contracts into having the force of federal law behind them, it will assuredly leave holes in consumer privacy rights because federal enforcement agencies will have no effective way to compel service providers or third parties to comply with the law. To avoid this, a federal privacy framework must create effective federal statutory obligations that hold each party accountable.

E. Correct Imbalances in Financial Privacy Law to Meet Consumers' Expectations

In our American society that relies on fast and convenient commerce, successful businesses serve customers as they expect and strive to accept a variety of forms of payment that meet customer needs. Most Main Street businesses, for example, accept credit and debit cards for the purchase of goods and services they provide. Increasingly they also accept other forms of payments, like consumers' using virtual cards in "wallets" on their mobile phones to make purchases in person and using digital payments from popular financial technology (fintech) companies online. Main Street businesses can accept those payments by securely interfacing with and sharing payment data with payment processors, card companies and banks authorizing payments.

We have concerns about any exemptions for financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) from comprehensive privacy legislation. Privacy legislation should ensure the payment data required to be shared in the financial system is protected equivalently by other parties, such as payment processors, payment networks and financial institutions.

GLBA was enacted in 1999, and its provisions are far outdated by decades of improvements in data privacy laws that render GLBA stale by comparison. MSPC supports efforts in the House Financial Services Committee to update GLBA because, in its present form, it does not provide consumers with *equivalent* privacy protections they would expect from enacted state privacy laws.

To illustrate the disparity between today's most referenced privacy laws to what financial institutions face under GLBA, the chart in *Appendix C (attached)* compares GLBA's provisions to the base privacy protections in privacy laws established by the European Union (which applies the General Data Protection Regulation to banks serving European customers) and in California (which exempts banks from the California Consumer Privacy Act). The chart demonstrates where GLBA does not include anything approximating the data privacy protections that most consumers have now come to expect after two and a half decades of improvements in this area of the law to protect consumer privacy. Most Americans would be surprised to learn they have far more privacy protections when buying an ice cream cone than when engaging in sensitive financial transactions involving their life savings with their financial institution. That simply should not be the outcome of federal privacy law and it is an area where Congress can improve on the state laws.

Congress has the opportunity to correct this imbalance in federal law when passing comprehensive privacy legislation to protect consumers' privacy in an equivalent manner when they purchase goods and services across the American economy.

III. Preserve Customer Loyalty Rewards and Benefits

A federal data privacy law must preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships like immensely popular customer loyalty, rewards, premium features, discounts or club card programs.

Loyalty programs are a critical and ever-growing facet of today's business models employed by a wide range of American businesses serving consumers in their daily lives. These programs are not to be mistaken with the principal business model of "free" online services that are paid for by commercial advertising, but rather are programs designed to provide discounts or rewards to a company's best customers to encourage future engagement with the same business when purchasing goods like food, apparel, or gas, and services like flights, hotel rooms, or rental cars. These programs are already inherently privacy-protective because they typically require customers to affirmatively opt into the plan in order to receive discounts, rewards, or other benefits as a member of the program.

Americans greatly benefit from customer loyalty programs offered by Main Street businesses. Bond Brand Loyalty Inc. has issued reports on loyalty programs and benefits to consumers for the past 14 years. In prior years, their reports found that 73% of consumers said they were more likely to recommend brands with good loyalty programs and 79% said loyalty programs make them more likely to continue doing business with the brands offering them.[5]

More recently, *The Bond Loyalty Report 2024* found that brands "using loyalty programs *well*...focused on personalization and superb customer care—both essential aspects of successful loyalty programs." As highlighted in Bond's press release, "participants must be

[5] See *The Loyalty Report 2019*, published by Bond Brand Loyalty, Inc.

'recognized' to feel seen, leaning into the human-to-human connections that leave them feeling special." Bond also found consumers join a "huge number of programs" as the average person participates in 19 different loyalty plans that influence their brand choices. "The influence of loyalty programs on customer behavior is higher than ever with 79% of consumers being more likely to recommend brands with solid loyalty programs and 85% of consumers saying they are more likely to continue buying from the brand."[6]

State privacy laws appropriately preserve customer loyalty programs but do so with very narrowly tailored provisions that do not alleviate businesses from the transparency, disclosure, and other provisions of state laws that provide consumer rights. Nor do state laws exempt providers of these programs from the laws' general prohibitions on retaliating against a consumer for exercising privacy rights. These state laws instead include savings clauses that indicate the prohibitions on retaliating or discriminating against consumers who exercise privacy rights cannot be construed to prohibit businesses from offering customers the ability to voluntarily participate in customer loyalty programs providing better prices or services. In short, they clarify that when some customers choose to participate in these programs, their individual choices cannot be viewed as an act of discrimination against any customer who does not choose to participate in the program.

MSPC strongly urges Congress to adopt provisions in federal privacy laws similar to the strong consensus of state laws that preserve loyalty programs and benefits where consumers voluntarily participate in *bona fide* programs offering better prices and services.[7]

IV. Ensure Reasonable Data Security Standards

MSPC supports federal privacy laws that ensure all businesses handling consumer data have reasonable data security standards appropriate to their size, nature of business, and scope of transactions involving personal data. We also support legislation designed to provide uniform federal rules for data security breach notification.

Consumer-facing companies like Main Street businesses must comply with data breach notification laws in all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. However, many of these laws exempt third-party service providers and financial institutions from the same breach notification requirements. Federal privacy law should correct these "breach notice holes" by requiring *all* businesses handling personal data to provide notice to affected individuals of their *own* data security breaches when they occur unless the non-breached party elects to notify individuals of a breach by a third-party processor. This approach would hold accountable *all* breached entities and create proper incentives for third parties to secure personal data they process on behalf of another business while preventing the shifting of notice obligations onto non-breached businesses.

---

[6] *See* Press Release, Bond Brand Loyalty Inc. (July 25, 2024)*:* https://info.bondbrandloyalty.com/the-loyalty-report-2024-press-release

[7] These laws use a savings clause clarifying that the state law's anti-retaliation or non-discrimination provisions shall not be construed to prohibit a business from offering better prices or services in connection with bona fide loyalty programs.

V. Establish Effective Accountability and Enforcement

Effective enforcement of a federal privacy law requires holding accountable *all* businesses handling personal data to *equivalent* data privacy standards using the same or similar enforcement mechanisms, thereby creating an even playing field and proper incentives across industry sectors to comply with those standards. Additionally, because "mistake-free" compliance is unlikely in this complex area of law, we support the approach adopted in all enacted state privacy laws of coupling *exclusive* governmental entity enforcement with the regulated entity's ability to correct or "cure" non-compliant practices within a limited period of time after receiving specific notice from the enforcement authority.

A. Benefits of *Exclusive* Governmental Entity Enforcement

Every enacted state comprehensive data privacy law relies on *exclusive* government enforcement coupled with a notice-and-cure provision. No comprehensive state privacy laws permit private rights of action to enforce the *privacy* provisions of those laws, even in California. Three critical reasons explain why this approach has developed into the appropriate consensus method for ensuring uniform application, interpretation, and enforcement of privacy standards under state privacy laws:

- Meaning of "Reasonable." All comprehensive state privacy laws contain dozens of uses of the words "reasonable" or "reasonably" when setting forth business obligations. Each use of those terms raises the possibility of widely different interpretations in meaning. Leaving private lawsuits to define what are "reasonable" privacy practices would result in endless litigation and differing standards that would call into question even the practices that government enforcement authorities find reasonable. It would also chill investment in innovative, responsible business practices that improve service to customers in a rapidly evolving technology environment. Exclusive governmental enforcement is the only way to ensure uniform interpretation and enforcement of the law.[8]

- Robust Compliance with Privacy Laws and Rapid Error Correction. To protect consumers, there must be a mechanism to encourage regulated entities to rapidly correct errors to get their privacy compliance right. All state privacy laws have adopted a notice-and-cure mechanism for this purpose, especially when a law is new. It provides an expedited means for businesses to correct technical errors without fearing bankrupting lawsuits. The California Attorney General confirmed the benefits of its notice-and-cure provision reporting that 75% of the

[8] In the Vermont Senate debate on June 17, 2024 (*see* webcast starting at 09:29) that sustained Governor Scott's veto of H. 121, the Vermont Data Privacy Act that included private rights of action, a key argument to sustain the veto (i.e., kill the bill) was that the bill had approximately 70 uses of the terms "reasonable" or "reasonably" that could not be left to private litigation in state courts to uniformly interpret and enforce. The Vermont Attorney General and other state AGs, however, could bring uniformity to the analysis. (Note: In California, there is joint AG and privacy agency enforcement authority, but it is still exclusively governmental enforcement authority of the privacy provisions of the California Consumer Privacy Act).

businesses notified had corrected their errors within 30 days.[9] Adversarial litigation, on the other hand, can take years and is not the best mechanism to encourage or achieve uniform, consistent, or timely compliance with the law.

- Private Litigation Disproportionately Impacts Main Street Businesses. Private rights of action have been rejected in every one of the states that have enacted comprehensive privacy laws. Private litigation often disproportionately impacts Main Street businesses, such as when plaintiff attorneys use "sue-and-settle" campaigns aimed at thousands of small businesses to collect quick settlements for vague, alleged violations of federal law. Dominant technology companies can force arbitration or otherwise fight litigation; small Main Street businesses cannot. Congressional committees have witnessed problems with so-called litigation trolls in many areas of law and passed legislation to stop it.[10] There is a significant risk that a similar cottage industry of *privacy* trolls, if given the chance, would leverage private rights of action against Main Street businesses in bad faith here as well.[11] Finally, as MSPC raised in its letter opposing private rights of action in the APRA, federal privacy legislation can risk disproportionately impacting Main Street businesses when exempting other parties from the same type of enforcement.[12]

~

Thank you for your consideration of MSPC's testimony. We appreciate the opportunity to participate in today's hearing and welcome your questions.

---

[9] California Attorney General Bonta reported that, in the first full year of implementing a notice-and-cure provision, 75% of companies notified of potential violations responded by amending their practices to come into compliance within the 30-day cure period, with the remaining 25% either in the process of their 30-day cure period or under further investigation. *See:* https://iapp.org/news/a/california-attorney-general-offer-ccpa-enforcement-update-launches-reporting-tool

[10] To curb the pattern or practice of sending vague and abusive demand letters alleging, in bad faith, patent infringement by Main Street and other businesses, the House Energy and Commerce Committee approved and reported to the House floor H.R. 2045, the *Targeting Rogue and Opaque Letters (TROL) Act*, to protect these businesses from the deceptive acts and practices of patent trolls.

[11] In the previously discussed Vermont Senate vote to sustain the governor's veto of the legislation with private rights of action *(see footnote 12)*, another compelling argument raised in opposition to private rights of action was that Vermont small businesses would be disproportionately impacted by out-of-state trial lawyers, driving up prices for consumers.

[12] The APRA exempted service providers and third parties from almost all enforcement by private rights of action while subjecting all Main Street businesses to this mass litigation threat, creating a severely disproportionate impact on some businesses over other and picking winners and losers in the marketplace.

Main Street
PRIVACY COALITION

MSPC Testimony to Senate Subcommittee on Privacy, Technology and the Law

Appendix A

Main Street Principles for Data Privacy Legislation

American businesses have no higher priority than earning and maintaining trusted relationships with their customers. To preserve those relationships, businesses must protect and responsibly use the personal information that customers share with them. As Congress considers legislative and regulatory solutions to address data privacy concerns, our coalition urges adoption of the following principles.[1]

- **Establish a Uniform National Privacy Law**
  Congress should enact a privacy law that benefits consumers and businesses alike by ensuring *all* personal data is protected in a consistent manner regardless of where a consumer resides.
- **Protect Consumers Comprehensively with Equivalent Standards for All Businesses**
  Federal data privacy law should apply requirements to all industries that handle personal data. A federal privacy law should not place a disproportionate burden on certain sectors of the economy while alleviating others from providing equivalent protections of personal data.
- **Create Statutory Obligations (Not Contractual Requirements) for All Entities that Handle Consumers' Data**
  Given imbalances in contractual negotiating power, effective consumer protection cannot be achieved by relying on Main Street businesses to regulate the conduct of market-dominant service providers through contracts. Service providers and third parties must have statutory privacy obligations when offering data processing, transmission, storage, or other services to collectively millions of Main Street businesses.
- **Preserve Customer Loyalty Rewards and Benefits**
  A federal privacy law must preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships such as loyalty programs.
- **Require Transparency and Customer Choice for All Businesses**
  Consumers deserve to know the categories of personal data that *all* businesses collect, how it is generally used to serve them, and the choices they have regarding those uses.
- **Hold Businesses Accountable for their Own Actions**
  Privacy legislation should not include terms that potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of an independent business owners.
- **Ensure Reasonable Data Security Standards**
  Privacy legislation should include reasonable data security standards for *all* businesses handling consumer data, as well as uniform rules for *any* businesses suffering a data security breach to notify affected individuals.
- **Establish Effective Accountability and Enforcement**
  Effective enforcement must hold accountable *all* entities handling personal data to *equivalent* data privacy standards using the *same* enforcement mechanisms, thereby creating an even playing field and proper incentives across industry sectors to comply with those standards. Because "mistake-free" compliance is unlikely in this complex area of law, we support the approach adopted in all enacted state privacy laws of coupling *exclusive* governmental entity enforcement with the regulated entity's ability to "cure" non-compliant practices within a limited period of time after timely and specific notice from the governmental authority.

[1] MSPC's principles for federal privacy legislation are also available at: https://mainstreetprivacy.com/principles/

MSPC Testimony to Senate Subcommittee on Privacy, Technology and the Law

Appendix B

Comparison of Processor Requirements in Three Key State Privacy Laws that Set the New Standard

- The chart below compares the processor requirements in the three key state privacy laws that were enacted early and set the standard for processor requirements: Virginia, Colorado, and Connecticut. These states passed laws in 2021 and 2022, after California's 2018 California Consumer Privacy Act (CCPA), which *failed to establish* any data processor requirements to protect consumers' data.
- Without statutory processor requirements, small-business controllers would lack the bargaining leverage necessary (in contractual negotiations with much larger data processors) to require processors to ensure the privacy of the controller's customer data when in the processor's hands.
- These key state privacy laws established a strong model that influenced most other state privacy laws, which adopted similar processor requirements to protect consumer data.

✓=Required ☒=Not Required KEY STATES THAT REQUIRED PROCESSORS TO:	VIRGINIA CDPA (2021)	COLORADO CPA (2021)	CONN. SB 6, Sec. 7 (2022)
Ensure Processor's Own Data Security when handling Controller's personal data	☒	✓	☒
Assist Fulfilling Privacy Rights Requests from Individuals and w/ Data Breach Notices	✓	✓	✓
Give Info to Controller to Complete DPAs (Data Privacy Assessments) Required of Controller	✓	✓	✓
Ensure Confidentiality of Personal Data by Processors' Employees w/ Personal Data	✓	✓	✓
Hold Subcontractors to Processor's Terms / Give Controller the Right to Object to Subs	✓/☒	✓/✓	✓/✓
Return/Delete Personal Data at Contract End (at the Choice of the Controller)	✓	✓	✓
Provide Controller Compliance Info Needed to Demonstrate Processor's Legal Compliance	✓	✓	✓
Allow and Cooperate w/ Reasonable Audits or Assessments at the Request of Controller	✓	✓	✓
Respect Cross-Liability Protections (Parties Not Liable for Another Party's Violations of their Own Obligations under the Act)	✓	✓	✓

MSPC Testimony to Senate Subcommittee on Privacy, Technology and the Law

Appendix C

Data Privacy Frameworks Adopted by European Union and California, Compared to GLBA Applying to U.S. Financial Institutions

PRIVACY LAW COMPARISON CHART

Consumer Privacy Rights regarding their Personal Information	GDPR (2016)	CCPA (2018)*	GLBA (1999)	Notes
Transparency	✓	✓	!	GLBA: partial transparency; only annually-*mailed* disclosure notice of data uses (w/ some exceptions)
Control (Choices)	✓	✓	✗	GLBA: no meaningful control; opt out *only for* non-affiliate sharing that is not excepted (e.g., some marketing)
Access	✓	✓	✗	
Correction	✓	✓	✗	
Deletion	✓	✓	✗	
Portability	✓	✓	✗	
Breach Notification	✓	!	!	CCPA: CA breach law requires notice, but not CCPA GLBA: Not required (guidance *only* says "should" notify)
Opt-Out of Direct Marketing	✓	✗	✗	GDPR: opt out of processing for direct marketing GLBA: joint marketing agreements override opt-out
Opt-Out of Data Sharing for Targeted Ads	✗	✓	✗	CCPA: opt out of data sharing to third parties for purposes of processing data for targeted advertising
Opt-Out of Data "Sales"	✗	✓	✗	CCPA: opt out of data "sales" to third parties for purposes beyond marketing/advertising (w/ some exceptions)

**CCPA, as amended by CPRA (2020)*

Testimony of Joel Thayer
President of Digital Progress Institute
Before the
The U.S. Senate Judiciary Privacy, Technology, and the Law
"Protecting the Virtual You: Safeguarding Americans' Online Data"
Wednesday, July 30, 2025

Thank you, Chairwoman Blackburn, Ranking Member Klobuchar, and esteemed members of this committee, for inviting me to testify and holding this important hearing.

My name is Joel Thayer, and I am the president of the Digital Progress Institute—a think tank based in Washington, D.C. focused on advancing bipartisan policies in the tech and telecom space. Ensuring privacy for all is a founding principle of the Institute and, as such, I very much appreciate this committee's commitment to building out a privacy framework that further assures that the integrity and ownership of our digital selves remains in our domain; not by companies with a domain name.

The concept of privacy is foundational to our constitutional democracy. Indeed, the Fourth Amendment prevents unlawful searches and seizures.[1] The Fifth Amendment prevents self-incrimination.[2] The First Amendment prevents the government from compelling Americans from making disclosures.[3] Some states, like Montana, explicitly list the right to privacy in their constitutions.[4]

Although our right to privacy from our government is well established, that is unfortunately not the case with respect to companies. With the allure of free services, we provide details about our most intimate selves to trillion-dollar tech companies who, in turn, make an enormous profit off the data they collect.

They know everything about us. What we like to eat. When we sleep. Where we live. Where we are. Our beliefs. Our fears. Curiously, they claim our age confounds them, but let's set that aside.

---

[1] U.S. Const. amend IV.
[2] *Id.* at amend. V.
[3] *NAACP v. Alabama*, 357 U.S. 449 (1958) (holding that the First Amendment protected the free association rights of the National Association for the Advancement of Colored People and its members).
[4] Mont. Const. art. II, § 10.

Worse, a recent Pew Study shows that 73% of Americans feel they have limited to no control over how companies use their personal information.[5] And the reality is they don't. We sign privacy policies that are filled with so much legal jargon that it may as well be unintelligible to the average person and—presto!—our data is now their data.

The problem is not just that they sell our data to third-party advertisers but also to those who use our data to create fake images, curate biased newsfeeds, conduct elaborate scams, and even engage in espionage. In short, we are not in control, and Americans are right to be concerned.

And with the advent of AI, this trend will only increase.

It makes the need for a national privacy framework preeminent because our current system is unsustainable. Even though many states, like California and Texas, have passed comprehensive privacy laws, we still need federal action to ensure we hold these companies accountable.

To be sure, tech behemoths view privacy violations as a mere cost of doing business, with penalties akin to a parking violation given their bottomless coffers. To demonstrate how some privacy laws have been of little help to consumers, let's get specific. Consumers sued Apple under California's privacy law, in part, for sharing recorded conversations that included personal health information with their physicians to medical ad companies.[6] Apple's surveillance and recordings covered conversations spanning a little under a decade. The case settled. So, what was the total cost of Apple giving advertisers an inside perspective on doctor-patient relations? A meager $95 million, which accounts for about 9 hours of Apple's annual profit.[7] And consumers won't see about a third of that, as it's reserved for the lawyers.

The reality is that if these Big Tech companies cared about user privacy, they would protect it. For instance, Google,[8] Amazon,[9] and Apple[10] can stop lowering their privacy protocols for autocratic regimes, such as the Chinese Communist Party, that seek to use their platforms to spy on consumers. Even better, Google can simply stop manipulating users' privacy settings on their devices and third-party services, which is already illegal.[11] Meta could stop unlawfully capturing

---

[5] Colleen McClain, Michelle Faverio, Monica Anderson, & Eugenie Park, *How Americans View Data Privacy*, Pew Research (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[6] *Lopez, et al v. Apple Inc.*, No. 19-04577, (N.D. Cal); *see also*, *Lopez, et al v. Apple Inc.*, No. 4:19-cv-04557-JSW, Second Amended Complaint, Doc. No. 70, paras. 38-43 (Mar. 17, 2021).
[7] Jonathan Stempel, *Apple to Pay $95 Million to Settle Siri Privacy Suit*, Reuters (Jan. 2, 2025), https://www.reuters.com/legal/apple-pay-95-million-settle-siri-privacy-lawsuit-2025-01-02/.
[8] Jack Poulson, *I Used to Work for Google. I Am a Conscientious Objector*, N.Y. Times (Apr. 23, 2019), https://www.nytimes.com/2019/04/23/opinion/google-privacy-china.html.
[9] Steve Stecklow & Jack Dastin, *Amazon Partnered with China Propaganda Arm*, CNBC (Dec. 17, 2021), https://www.cnbc.com/2021/12/17/amazon-partnered-with-china-propaganda-arm.html.
[10] *Inside Apple's Comprmises in China: A Times Investigation*, N.Y. Times (Jun. 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.
[11] *In re Google Assistant Privacy* Litigation, No. 19-cv-04286-BLF (N.D. CA 2024), https://www.googleassistantprivacylitigation.com/ (alleging that Google Assistant can activate and record communications even when a user does not intentionally trigger Google Assistant with a hot word, like "Okay

and using personal biometric data.[12] Apple describes user privacy as a "human right," but, in reality, it treats user privacy less as a fundamental human right and more as a license to collude with Google and other Big Tech firms to monetize and monopolize every facet of its users' data, lives, and privacy.

It is no wonder why that 85% of people want more to be done to protect user privacy.[13] We need government intervention here.

The good news is that protecting privacy is a bipartisan issue. Indeed, 20 states across the political spectrum have passed privacy laws. And, as evidenced by this hearing, Congress appears poised to address the issue again. The Institute welcomes this much-needed development.

With that in mind, here are a few high-level suggestions as the Committee evaluates paths forward:

First, define your goals and keep the framework targeted at accomplishing its goals. One of the primary issues with previous attempts at passing meaningful privacy laws has been that bills attempt to do too much all at once. We have seen the most success in legislation that has clearly articulated goals with targeted solutions. It is why the Institute has supported targeted, bipartisan measures, such as the Protecting Americans from Foreign Adversary Controlled Applications Act, TAKE IT DOWN Act, Kids Online Safety Act, and App Store Accountability Act to name a few.

As we have seen in the E.U.'s General Data Protection Regulation (GDPR), overly sweeping privacy laws have the unintended consequence of entrenching incumbents. The GDPR should be a cautionary tale for the U.S., because it clearly shows that privacy regulations without market guardrails can seriously exacerbate today's competition issues we have with Big Tech. For example, the European Centre of Economic Policy Research found that "[w]ith the introduction of GDPR, the dominant firm in many markets for web technologies, Google, increases its market share whereas all other firms that supply web technology either do not see a change in market share or suffer losses…"[14] The primary reason is that the tech market is highly vertically

---

Google," or manually activate Google Assistant on their device); *see* also, Erik Sherman, *Is Google Ignoring Internet Privacy?* CBS News (Feb. 22, 2012), https://www.cbsnews.com/news/is-google-ignoring-internet-privacy-update/.

[12] The Office of the Attorney General of Texas, *Attorney General Ken Paxton Secures $1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data In Largest Settlement Ever Obtained From An Action Brought By A Single State*, Press Release (Jul. 30, 2024), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture.

[13] Exploding Topics, *23+ Alarming Data Privacy Statistics for 2025*, Blog (Jun. 5, 2025), https://explodingtopics.com/blog/data-privacy-stats.

[14] Peukert, C, S Bechtold, M Batikas and T Kretschmer, *DP14475 European Privacy Law and Global Markets for Data*, CEPR Discussion Paper No. 14475. CEPR Press, Paris & London (2020). https://cepr.org/publications/dp14475.

integrated where smaller companies are inextricably reliant on these larger platforms to either house their data, host their apps or even promote their services on those Big Tech platforms.

Second, enforcement matters. In our experience, agency actions or attorney general enforcement are the most effective. For instance, the Texas Attorney General recently secured a $1.345 billion settlement against Google "for unlawfully tracking and collecting users' private data regarding geolocation, incognito searches, and biometric data."[15] As should be obvious, that's $1.345 billion that *only* covers the people of Texas. Contrast that with the Apple case discussed earlier with a settlement of only $95 million covering the entire country. In other words, a private right of action may behave more as a carrot as opposed to a stick given these companies seemingly endless teams of lawyers and budgets. What's more, agencies can tailor their remedies more precisely to protect American citizens. For example, COPPA permits the Federal Trade Commission to promulgate rules and impose injunctive relief to enjoin certain data collection with respect to users under the age of 13.[16] The Institute strongly encourages the committee to evaluate those options and possibly targeted agency rulemakings so as to prevent the overly prescriptive technical statutes.

Third, the broader the federal statute, the more important preemption will become. That's because targeted legislation is less likely to run into differing state regimes, whereas 20 states have now passed some form of comprehensive privacy legislation. The Institute recommends that any preemption framework should be clear on what it is preempting and should reserve rights for state attorney general enforcement. Key areas ripe for preemption are developing basic definitions (*e.g.*, "personal information"), the creation of data rights, and what specific data management practices are to be prohibited.

Once again, I would like to thank the sub-Committee for allowing me to testify and I welcome any questions you may have.

Sincerely,

Joel L. Thayer
President & Member of the Board

---

[15] The Office of the Attorney General of Texas, *Attorney General Ken Paxton Secures Historic $1.375 Billion Settlement with Google Related to Texans' Data Privacy Rights*, Press Release (May 9, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-historic-1375-billion-settlement-google-related-texans-data.

[16] 15 U.S.C. § 57a; *see also* 15 U.S.C. § 6502.

Senate Judiciary Subcommittee on Privacy, Technology and the Law
"Protecting the Virtual You: Safeguarding Americans' Online Data"
Questions for the Record for Ms. Kate Goodloe

Questions from Senator Blackburn:

1. What features make certain state privacy laws more effective than others?

To be effective, a privacy law must place meaningful limits on businesses that handle consumers' personal data and require them to handle that data responsibly.

These limits must reflect the company's role in handling consumers' personal data. Specifically, a privacy law must distinguish between two types of companies: (1) controllers, which decide why and how to collect a consumer's data, and (2) processors, which handle data on behalf of another company and pursuant to the company's instructions.

All 20 state privacy laws distinguish between controllers and processors and assign strong — but different — obligations to each type of company.[1] This distinction dates back more than 40 years and is critical to modern privacy laws worldwide. Both controllers and processors have important responsibilities to protect consumers' data, but their obligations should fit their roles. If legislation does not reflect these different roles, it can end up undermining the goal of improving consumer privacy by creating obligations that inadvertently pose new privacy and security risks for consumers.

For controllers, state privacy laws assign obligations that focus on the controller's decisions to collect and use consumers' personal data. These include requiring controllers to:

- Ask for consent if they will process sensitive data.
- Minimize the amount of personal data they collect and use, in line with data minimization requirements.
- Respond to consumer rights requests to access, correct, delete, and port data, and requests to opt-out of activities like targeted advertising, sale of data, and certain types of profiling.

For processors, state privacy laws assign obligations that reflect their role in handling data on behalf of a controller. These include requiring processors to:

- Process personal data pursuant to a contract with the controller.
- Handle that data confidentially.
- Assist the controller in responding to consumer rights requests for data held by the processor, and provide information the controller needs to conduct a privacy impact assessment.

2. Given the proliferation of state privacy laws, what type of preemption should a federal data privacy law adopt?

BSA supports a federal privacy law that is worthy of preempting existing comprehensive state consumer privacy laws and ensures a consumer's privacy rights do not depend on the state in which she lives.

---

[1] Nineteen states use the terms controller and processor, while California uses the terms business and service provider.

We recognize that states have been leaders in adopting new privacy protections. However, navigating a growing number of state-level obligations creates significant challenges for companies that operate nationwide and creates confusion for consumers about how and when their rights apply.

Importantly, the aim of a consistent national standard is not to weaken privacy protections already provided by comprehensive state consumer privacy laws. A federal law should replace, but not undermine, those state privacy laws — and extend the protections already adopted in 20 states to consumers across the country. A federal law should also ensure that states continue to be leaders in enforcing privacy protections, by ensuring that a federal privacy law empowers state attorneys general to enforce its obligations.

More broadly, adopting a privacy law will strengthen trust in technologies. That is important to the economy broadly, and to our members specifically. In July 2025, BSA released an agenda on AI adoption, which emphasizes that clear regulatory frameworks and practical governance structures are critical to build customer confidence and promote adoption of technologies. That sort of adoption is a national economic priority.

For these reasons, BSA supports a federal privacy law that preempts existing comprehensive state consumer privacy laws and creates a single, national standard that protects consumers nationwide.

3. **In your opening statement, you discussed that different companies should be required to handle consumers' personal data responsibly, but each company must take different actions to protect consumers as they play different roles in handling their data. Taking this idea a step further, should different categories of personal data be treated differently? For example, are heightened protections needed for more sensitive user information like financial information, health information, precise geolocation information or even the content of communications?**

Yes, a privacy law should create heightened protections for sensitive personal data. At the state level, for example, 16 of the 20 comprehensive state consumer privacy laws require companies to obtain a consumer's affirmative consent to process sensitive data. California is one of the only states to not create such protections, but instead creates a right for consumers to ask companies to limit how they use and disclose sensitive personal information that is collected about them. A national privacy law should create important protections for the sensitive personal data of Americans nationwide.

4. **The Internet of Things or IoT seamlessly connects everyday devices to the internet and enables them to send and receive data. This innovation simplifies life and boosts efficiency across various sectors, including health care, agriculture and home life. What additional privacy concerns does data collected from these smart devices such as wearable medical devices, smart lights, or thermostats create as compared to data collected through more traditional methods such as mobile and computer devices?**

Consumers share personal information every day, just by using routine products and services that make their lives easier. In some cases, this includes Internet of Things devices, which may collect personal data about the consumers using those devices.

We need a national privacy law that ensures there is a clear standard for protecting the privacy of American consumers' personal data. A federal privacy law will create broad protections that address how companies can collect and use consumers' personal data, including in a range of scenarios raised by IoT devices.

A privacy law should create new rights for consumers, including the rights to access, correct, delete, and port their data. This can help consumers understand what types of data companies are collecting and using — and allow them to ask for their data to be deleted. Privacy laws also limit how and why companies collect personal data in the first place and can ensure companies do so in line with consumer expectations. These rules are important because consumers should be able to trust that their personal information will be used responsibly. A privacy law that creates responsible safeguards for the collection and use of consumers' personal data will increase consumers' trust and promote adoption of technology.

5. What is the role of data minimization in a privacy law, and which types of companies should be subject to a data minimization obligation?

Data minimization requirements are an important part of privacy laws. By minimizing the amount of consumers' data that companies collect and use, these obligations can limit the amount of data that is exposed to privacy or security risks.

We urge policymakers to focus on two aspects of data minimization obligations.

First: Any data minimization requirement must leave room for companies to responsibly improve existing products and develop new ones. If a privacy law does not allow companies to process personal data to improve and develop products, it can inadvertently freeze technologies where they exist today. Data minimization obligations need to recognize that companies should be able to process personal data to improve existing products and develop new ones in ways that consumers expect. This is important to ensure that products and services improve over time, to the benefit of all consumers. A privacy law needs to adopt safeguards that achieve this goal.

Second: Data minimization obligations must apply to controllers, since they are the companies that decide how and why to collect consumers' personal data. Those decisions must implement obligations to minimize the collection and use of personal data in the first place. All comprehensive state consumer privacy laws take this approach and apply data minimization obligations to controllers. Processors, in turn, are already subject to strict limits on how they handle consumers' data — since by definition processors can only process personal data on behalf of a controller and pursuant to its instructions.

If a privacy law took a different approach and applied a freestanding data minimization obligation to processors, it would actually undermine the goal of minimizing access to consumers' personal data by increasing the amount of companies accessing that data. For example, a cloud storage company may act as a processor for hundreds of businesses. The cloud provider does not dig through its customers' data to understand why each business collects specific types of personal data or the purposes for which each type of data is processed. Its job is to keep that data secure, not to review it. If the cloud provider were subject

to a freestanding data minimization obligation, it may have to start behaving as if it 'owned' the data entrusted to it by its business customers and review that data to understand if its business customers minimize their collection and use of consumers' data. That doesn't make sense and undermines the goal of minimizing access to consumers' data. Instead, the right set of limits already exists for processors, which by definition can only process personal data on behalf of a controller and pursuant to its instructions.

Senate Judiciary Subcommittee on Privacy, Technology and the Law
"Protecting the Virtual You: Safeguarding Americans' Online Data"

Questions for the Record for Mr. Paul Martino,
General Counsel to the Main Street Privacy Coalition
Responses Submitted August 21, 2025

Questions from Senator Blackburn:

1. **Businesses today face an increasing challenge of how best to use consumer data without violating various state privacy laws. Today, we have heard about the difference between first- and third-party data. A third kind of data is known as "zero party data." Zero party data is information a customer intentionally and proactively shares with a business. One of the largest methods businesses collect zero party data is through Loyalty Programs. Can you describe some of the ways members of the Mainstreet Privacy Coalition are using data to enhance the customer experience?**

Main Street businesses use customer data for a variety of purposes to better serve their customers as they expect to be served and enhance their experience.

Much of the consumer data that is provided by customers to Main Street businesses is relied on by these businesses to provide the services customers expect. For example, Main Street businesses may use data to ship products purchased online to their customers, enable customers to create gift registries or wish lists, have records of customers' purchases to enable returns and exchanges of products, reserve hotel and resort rooms, make restaurant reservations, provide customer loyalty benefits or enhanced services, and similar expected business uses that serve customers' needs today.

Loyalty programs, for example, are a critical and ever-growing facet of today's business models employed by a wide range of American businesses serving consumers in their daily lives. These programs are designed to provide discounts or rewards to a company's customers that encourage future engagement with the same business when purchasing goods and services. These programs are already inherently privacy-protective because they require customers to affirmatively opt into a loyalty plan in order to receive discounts, rewards, enhanced services, or other benefits as a member of the program.

Studies have shown that Americans greatly benefit from customer loyalty programs offered by Main Street businesses. *The Bond Loyalty Report 2024* found that brands "using loyalty programs *well*…focused on personalization and superb customer care—both essential aspects of successful loyalty programs." Bond also found consumers join a "huge number of programs" as the average person participates in 19 different loyalty plans that influence their brand choices. "The influence of loyalty programs on customer behavior is higher than ever with 79% of consumers being more likely to recommend brands with solid loyalty programs and 85% of consumers saying they are more likely to continue buying from the brand."[1]

The Main Street Privacy Coalition believes a federal privacy law must preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships such as loyalty programs that enhance the customer experience.

---

[1] *See* Bond Brand Loyalty Inc. (July 25, 2024): https://info.bondbrandloyalty.com/the-loyalty-report-2024-press-release

Main Street Privacy Coalition
Responses to Questions for the Record
August 21, 2025

2. While there has been significant discussion around preemption of state privacy laws, how should a federal privacy framework account for existing federal and state industry specific laws like HIPAA in the healthcare industry or the Fair Credit Reporting Act in the financial industry?

The Main Street Privacy Coalition's principles for federal legislation state that federal privacy laws should require *equivalent* data privacy obligations for all businesses that handle consumers' personal information. We further recommend that federal privacy laws should not place a disproportionate burden on certain sectors of the economy while alleviating other sectors from providing equivalent protections of personal data.

Main Street businesses will bear the full burden of regulatory obligations under proposed federal privacy laws just as they do with all enacted state comprehensive privacy laws. Previous federal legislation, however, has often significantly narrowed the obligations of other businesses, in part through exemptions for federal and state industry-specific laws. These exemptions may be appropriate when they are provided for laws that comprehensively protect consumer privacy. However, some past bills have exempted businesses subject to federal laws that provide far less consumer privacy protections than are being required of Main Street businesses under the comprehensive state privacy laws and federal bills.

For example, we have raised concerns with exemptions related to businesses subject to the Gramm-Leach Bliley Act (GLBA), as further detailed in our written testimony. Main Street businesses must securely share sensitive payment data with financial institutions, card networks, and payment processors operating in the electronic payments system in the course of processing millions of digital payment transactions each day.

Consumers expect their privacy to be protected in the payments system. Main Street businesses also expect not to be held liable – or to be subject to public scrutiny – for any of the shortcomings of financial institutions, card networks, or payment processors that fail to protect the privacy of the shared payment information. Importantly, GLBA does not currently require the same level of privacy protection from these parties as other laws require of Main Street businesses. (See Appendix A for GLBA comparison chart.)

As shown in the attached comparison chart, GLBA was enacted in 1999 and its provisions are outdated. The past few decades have led to improvements in data privacy laws that render GLBA stale and inadequate by comparison. GLBA in its present form does not provide consumers with *equivalent* privacy protections that they would expect from the already enacted state privacy laws. Congress should update GLBA to the level necessary for its privacy protections to meet equivalent privacy standards that other industry sectors have adopted as part of any effort by Congress to enact comprehensive privacy legislation.

3. U.S. privacy protections are clearly fragmented across the states. A 2022 study conducted by the International Technology and Innovation Foundation found that over a 10-year period, compliance with 50 different state privacy laws would cost the US economy more than $1 trillion, with more than $200 billion of the compliance costs

Main Street Privacy Coalition
Responses to Questions for the Record
August 21, 2025

placed on small businesses. What are some of the challenges for businesses working in different states with different privacy laws?

Congress should enact a privacy law that benefits consumers and businesses alike by ensuring *all* personal data is protected in a consistent manner regardless of where in the nation a consumer resides or travels.

Americans expect their privacy to be protected the same, everywhere. Our coalition members share a strong conviction that a preemptive federal privacy law will benefit consumers and Main Street businesses alike. A single, uniform federal privacy law would give consumers confidence that their data will be protected the same way across America regardless of where they live or choose to do business.

Similarly, a uniform nationwide privacy law would provide Main Street businesses with the certainty they need to use data lawfully and responsibly to better serve their customers in all of their locations, online or across state lines. It would permit businesses to streamline compliance practices and internal processes through uniform privacy standards applicable to all customers that ensure their privacy rights requests, data disclosures, choices, and other important privacy protections are provided regardless of a consumer's location in the United States.

Some of the business challenges that a preemptive federal privacy law would help resolve relate particularly to smaller businesses on Main Street that may have a single physical location but provide goods and services to Americans online. These small businesses are currently held to the unworkable standard today of needing to comply with all state laws and regulations on consumer privacy in the varied locations of their online customers, in addition to the laws of the state in which their physical place of business is located.

Given Main Street businesses' need to maintain an online presence to compete in today's highly competitive markets, their privacy compliance costs naturally increase with each new state privacy law or regulation adopted in the existing patchwork of state laws. Main Street businesses must bear the costs associated with the increasing complexity of privacy laws that include new definitions, thresholds, and rules not seen before. In addition to complying with laws that vary greatly from their own state's law, they must often adopt new business processes and purchase data privacy services they haven't used before simply to comply with all other state laws to serve their customers online, wherever they are located.

Similar challenges are faced by small businesses with physical locations on each side of a state border. This occurs often and differing privacy regimes among states creates added compliance costs and burdens.

The Main Street Privacy Coalition strongly urges Congress to enact a nationwide privacy law that both improves and extends uniform privacy protections to all Americans across the United States while addressing the many challenges Main Street businesses face today complying with varying and increasingly complex privacy laws enacted in states outside their own state.

Main Street Privacy Coalition
Responses to Questions for the Record
August 21, 2025

Attachment A

Data Privacy Frameworks Adopted by European Union and California Compared to GLBA Applying to U.S. Financial Institutions

PRIVACY LAW COMPARISON CHART

Consumer Privacy Rights regarding their Personal Information	GDPR (2016)	CCPA (2018)*	GLBA (1999)	Notes
Transparency	✓	✓	!	GLBA: partial transparency; only annually-*mailed* disclosure notice of data uses (w/ some exceptions)
Control (Choices)	✓	✓	✗	GLBA: no meaningful control; opt out *only for* non-affiliate sharing that is not excepted (e.g., some marketing)
Access	✓	✓	✗	
Correction	✓	✓	✗	
Deletion	✓	✓	✗	
Portability	✓	✓	✗	
Breach Notification	✓	!	!	CCPA: CA breach law requires notice, but not CCPA GLBA: Not required (guidance *only* says "should" notify)
Opt-Out of Direct Marketing	✓	✗	✗	GDPR: opt out of processing for direct marketing GLBA: joint marketing agreements override opt-out
Opt-Out of Data Sharing for Targeted Ads	✗	✓	✗	CCPA: opt out of data sharing to third parties for purposes of processing data for targeted advertising
Opt-Out of Data "Sales"	✗	✓	✗	CCPA: opt out of data "sales" to third parties for purposes beyond marketing/advertising (w/ some exceptions)

**CCPA, as amended by CPRA (2020)*

Senate Judiciary Subcommittee on Privacy, Technology and the Law
"Protecting the Virtual You: Safeguarding Americans' Online Data"
Questions for the Record for Mr. Joel Thayer

Questions from Senator Blackburn:

1. **What features make certain state privacy laws more effective than others?**

Thank you for the question, Senator. I believe that laws that target specific actions are far preferable than those that seek to do too much all at once.

Take, for instance, Texas's privacy law, the Texas Data Privacy and Security Act (TDPSA).[1] It just focuses on targeted advertising. It requires businesses to offer consumers the ability to opt-out of having their data used for that purpose. The TDPSA also protects a narrow set of the most sensitive personal data. And it is triggered by selling the data. Those targeted protections allow everyone—companies, consumers, and the government—to know what is protected and what is not; and it gives the government strong authority to aggressively enforce those protections.

Laws that zero in on the harms you want to quell and the data you seek to protect yield much better results than those having very broad definitions and missions.

2. **There are many protections for children in the physical world. They can't walk into a strip club. They can't purchase alcohol and tobacco in a liquor store. But in the virtual space, they can access all these harms and more. What heightened protections should we consider when discussing the collection, processing, or transfer of children's data?**

To start, I'd like to acknowledge that you have been a champion on the issue of child online safety. Frankly, it is hard to find a much better fighter than you when it comes to parental empowerment and child protection.

But to your question, we need targeted legislation, such as your Kids Online Safety Act (KOSA) to disincentivize the practice of data collection on kids in the first place. If passed, KOSA would require social media companies to provide parents and adolescents with tools to help safeguard the experience of kids on social media. What's more, KOSA would impose a "duty of care" on platforms to ensure that they are not using design features made for adults on child users, such as algorithms pushing sexual exploitation material or violent videos to children. KOSA's duty of care provides attorneys general with a clear path forward to address these harms and keep Big Tech accountable when they hurt children.

Another step we can take is to recognize that we have laws intended to protect children online, such as the Children's Online Privacy Protection Act (COPPA), but that such laws have a big loophole: They only apply if an online platform has de facto actual knowledge of a user's age. One easy way to fix this problem is to enact a law with an adequate age verification requirement that ensures these companies meet the de facto actual knowledge standard. The App Store Accountability Act (ASAA) accomplishes this by requiring app stores to verify age and seek

[1] Tex. Bus. & Com. Code Ann. § 541.001 et seq.

parental consent when a child wants to use an app on their stores. This ensures that an app developer has actual knowledge of each user's age category (e.g., a child under COPPA). What is more, ASAA gives parents the ability to monitor what privacy policies and terms of service to which their kids are assenting and putting them back in the driver's seat. Additionally, ASAA protects this very age category data by prohibiting any app developer from sharing the age data received from app stores to third parties or they will face very hefty penalties.

Passing these two measures alone can go a long way to ensuring kids are protected online and platforms are prohibited from profiting off of them, which, in turn, protects their data and digital selves.

In sum, we are going to need a combination of policy solutions that removes the incentive of collecting kid data and punishes these companies when they do.

3. **My previous data privacy legislation, the BROWSER Act, looked at the tech ecosystem in a new way. It had one set of rules and one regulator – the FTC – for both broadband and what we used to refer to as "edge companies." In the eight years since I first introduced this bill, my colleagues have come around to see just why these tech companies need to be subject to data privacy regulation. In fact, the vast amounts of data they collect and consume on consumers is more than probably any other provider. With that in mind, are there any obligations that should look different for tech companies as opposed to others in the tech stack?**

Absolutely. You are just as correct now as you were eight years ago. Even though the common thread of each company is that they collect data, some in the tech stack are far more pervasive than others. This is especially true for those companies collecting personal information to sell digital advertisements. Big Tech firms, such as Apple, Google, Amazon, and Meta, have troves of personal data due to their vertical integrated services. This market concentration and insatiable need for data can spell out a disaster for the consumer, which should make these companies a strong target for any privacy legislation.

Just take Google as a prime example. Given that Google controls nearly 90 percent of the search market and all of that data are on its servers, one breach can be a national catastrophe.[2] Worse, because there is no feasible competitor to it, Google has no market incentive to put consumer privacy or even its consumers first. Frankly the fact that it has no true competitors gives Google more reason to continue violating users' privacy. There's no risk of consumer backlash; only the reward of more ad revenue.

And Big Tech companies collect very intimate data from their users. As I described in my testimony, Apple shared recorded conversations of personal health information with their physicians to ad companies. A jury found that Meta was unlawfully collecting sensitive health information via a third-party app that included female users' sexual health, gynecological health, and menstruation cycles.[3] And the list goes on.

---

[2] Jonathan Theuring & Katie Barnard, *Bing vs Google: Search Engine Comparison 2025*, Impression (updated Aug. 7, 2025), https://www.impressiondigital.com/blog/bing-differ-google/.
[3] *Frasco v. Flo Health*, Case No. 21-cv-00757-JT, Verdict Form, Doc. No. 756 (Aug. 4, 2025).

Worse, they may even share data with foreign adversaries. For example, hundreds of apps on Apple's App Store openly admit to providing sensitive data to China. Some even use Apple's ARKit, which enables apps to detect more than 50 unique facial expressions[4] and project 30,000 infrared dots[5] to create a 3D map of a user's face, while allowing the app to retain the data.[6] Apple even has China-based AI company Meitu's BeautyCam-AI Photo Editor on its App Store that uses the ARKit to extract "facial mapping information." Astonishingly, the app enjoyed 2 million downloads in one month.[7] Another China-based app called ProKnockOut-Cut Paste Photos uses Apple's ARKit and reveals that the "information will be stored in China" in its privacy policy.[8] Some of these apps admit to sending health data to China from Apple's HealthKit, which allows apps to collect more than 100 different data points across numerous categories. And it does not end there. China-based wellness app Wearfit Pro claims to access data from Apple's HealthKit and openly discloses that the "data will be stored in the territory of the People's Republic of China."[9] The app's privacy policy states that it collects users' "sleep, heart rate, blood oxygen, blood pressure, blood sugar, body temperature, weight, body age, heart rate and other data."[10]

These data interactions are just some of the issues involving tech companies, but undoubtably these issues are distinct from any other part of the Internet stack and warrant targeted legislation to quell. Congress would be right to have legislation focused on their particular data uses.

As I said in my testimony, we also need to establish data rights for Americans against these tech companies in particular. Congress could look to the TDPSA as a starting point. The TDPSA created the following digital rights:

1. The "[r]ight to know whether a company is processing the consumer's personal data and to obtain the personal data in a readable format;"
2. The "[r]ight to correct inaccuracies in the consumer's personal data, taking into account the nature of the data and the purposes for processing the data;"
3. The "[r]ight to delete personal data provided by or obtained about the consumer;"
4. The "[r]ight to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling…" in certain circumstances; and

---

[4] Apple Developer Guidelines, *Tracking and Visualizing Faces*, Apple (last visited Aug. 13, 2025), https://developer.apple.com/documentation/arkit/tracking-and-visualizing-faces.
[5] Jason Cipriani, *iPhone Face ID Is Pretty Cool. Here's How it Works and How to Use It*, CNET (Feb. 5, 2020), https://www.cnet.com/tech/services-and-software/the-iphone-and-ipads-face-id-tech-is-pretty-darn-cool-heres-how-it-works-and-how-to-use-it/.
[6] Stephen Nellis, *App Developers Access to iPhone X Face Data Spooks Some Privacy Experts*, Reuters (Nov. 2, 2017), https://www.reuters.com/article/us-apple-iphone-privacy-analysis/app-developer-access-to-iphone-x-face-data-spooks-some-privacy-experts-idUSKBN1D20DZ/.
[7] https://app.sensortower.com/publisher/ios/416048308?page=1&page_size=25.
[8] Shenzhen Qianhai Happy Tour Inc, Privacy Policy (last visited Aug. 13, 2025), https://privacy.biggerlens.cn/app/privacy?name=knockout-google&os=android&language=en.
[9] Wearfit Pro, Privacy Policy (last visited Aug. 13. 2025), https://h5.iwhop.com/login/privacy_policy/privacy_policy_en.html.
[10] *Id.*

5. The "[r]ight to not face retaliation or discrimination for exercising these rights."[11]

4. We have heard concerns about giving the FTC additional authority, whether through rulemaking or enforcement mechanisms, to regulate data privacy. There are certainly members who do not want to give the agency additional resources or change their existing statutory regime. What would you say to those that claim this is a problem?

I have heard those arguments and believe that such views misunderstand the authority that the FTC already has, which has included regulating privacy. The FTC Act allows the Commission to prohibit "unfair or deceptive acts or practices *in or affecting commerce*" and "unfair methods of competition *in or affecting commerce* [emphasis added]."[12] From a purely textualist perspective, that's quite an expansive remit.

Currently, the FTC seems to have ample authority to define deceptive practices under Section 5—in tandem with its Trade Regulation Rules (TRR) rulemaking authority pursuant to the Magnusson-Moss Warranty Act (Mag-Moss)—to include listing privacy violations as part of that definition. Indeed, during the Biden Administration, FTC Chair Lina Khan used its TRR rulemaking authority to promulgate rules to "protect people's privacy and information in the commercial surveillance economy."[13] And the FTC is sitting on a solid legal foundation to promulgate such rules. To be sure, when Congress enacted Mag-Moss, it gave the FTC the authority to issue TRRs related to unfair or deceptive acts or practices (UDAP) under a strict formal rulemaking procedure.[14] Better for the FTC's case, most of its privacy investigations and enforcement fall under its UDAP authority and courts have generally permitted the FTC to use that authority to do so.[15] Thus, so long as the FTC follows the procedures outlined in Mag-Moss, a court could likely uphold such rules without any further grants from Congress.

So, passing a specific authority statute, like a privacy law, would have the practical effect of limiting the FTC's jurisdiction on the subject, not expand the authority that it already possesses under Section 5. As the Supreme Court succinctly put it in *Morales v. Trans World Airlines, Inc.*: "[I]t is a commonplace of statutory construction that the specific governs the general."[16] In *HCSC-Laundry v. U.S.*, the Court further explained that courts ought to read the specific statute governing the general "particularly when the two are interrelated and closely positioned, both in

---

[11] Office of the Attorney General of Texas, *Texas Data Privacy and Security Act*, Website (last visited Aug. 13, 2025), https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/texas-data-privacy-and-security-act.
[12] 15 U.S.C. § 45.
[13] FTC, *Commercial Surveillance and Data Security Rulemaking*, Website (Aug. 11, 2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.
[14] 15 U.S.C. § 57a(1)(A)–(B).
[15] *E.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3rd Cir. 2015) (holding that a company's alleged failure to maintain reasonable and appropriate data security measures as an unfair practice under Section 5 of the FTC Act); *See* also, FTC, *Privacy and Security Enforcement*, Website (last visited Aug. 15, 2025), https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement#:~:text=Privacy%20and%20Security%20Enforcement%20When%20companies%20tell,FTC%20can%20and%20does%20take%20law%20enforcement.
[16] 504 U.S. 374, 385 (1992).

fact being parts of [the same statutory scheme]."[17] Better yet, the Ninth Circuit in *Roseman v. U.S.* determined that the specific statute controls over the general statute if the application of the general statute "conflicts" with the specific statute, especially if the specific authority was passed after the general statute.[18]

To illustrate how specific statutes interplay with general statutes, look no further than the Supreme Court's opinion in *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP* written by the late-Justice Scalia.[19] In that case, the Court considered whether a complaint alleging breach of the Verizon's duty under the 1996 Telecom Act to share its network with competitors states a claim under Section 2 of the Sherman Act.[20] Justice Scalia wrote that "a detailed regulatory scheme such as that created by the 1996 Act ordinarily raises the question whether the regulated entities are not shielded from antitrust scrutiny altogether by the doctrine of implied immunity."[21] In other words, a specific statute may have the effect of trumping the general antitrust statute's enforcement. What's more, Justice Scalia goes on to say that when there exists a "detailed regulatory scheme, it would behoove even courts to observe it over the general authority. Doing so may "avoid the real possibility of judgments conflicting with the agency's regulatory scheme…."[22]

Given this, legislation you have spearheaded, particularly KOSA and the Open App Markets Act (OAMA), would have the practical effect of narrowing the FTC's general authority. Both KOSA and OAMA would provide the FTC with specific statutes oriented towards particularized harms.

Let's start with KOSA. KOSA would specify the types of harms the FTC can regulate and investigate with respect to protecting kids online and, thus, limits (not expands) its Section 5's deceptive practices authority. Similar to what the Telecom Act did for the Sherman Act in *Verizon*, KOSA would narrow the FTC's Section 5 remit with respect to protecting kids from social media platforms and define what harms the FTC could investigate via KOSA's "duty of care" section that focused only on specific addictive functions. Without KOSA's duty of care, the FTC has free rein to decide what harms to minors look like in the broadest sense (think back to the text of Section 5).

The same is true with OAMA because it would limit its Section 5's unfair competition authority by specifying what competitive harms the FTC can police with respect to the app store market. Section 3 of OAMA articulates what competitive harms look like in the app-store market and would focus the FTC's remit to looking for specific anticompetitive behaviors. OAMA would prevent Apple and Google from forcing developers into particular exclusive dealings with them, interfering with developers' communications with their customers, using developers' non-public data to get an unfair competitive advantage over them, and using their search functions to bury apps. Any use of Section 5 to address competition in app stores in any other way would almost certainly conflict with the provisions of OAMA. Given the caselaw, OAMA would displace any attempt from the FTC to use its expansive Section 5 authority to circumvent it, which has the effect of narrowing it.

---

[17] 450 U.S. 1, 7 (1981).
[18] 364 F.2d 18 (9th Cir. 1966).
[19] 540 U.S. 398 (2003).
[20] *Id.*
[21] *Id.* at 407.
[22] *Id.*

Passing a privacy law with FTC enforcement can have the same effect as that of OAMA and KOSA.

In sum, these concerns are unfounded and are divorced from traditional notions of statutory construction.

5. **The GDPR was enacted nearly 10 years ago and there are currently 20 state privacy laws on the books, have you seen where tech companies are pulling specific services from states due to the cost of compliance?**

There is no evidence that any tech company—large or small—has decided to leave a market or failed to provide a service based solely on a privacy regulation.

Consider China's privacy law, the Personal Information Protection Law (PIPL). Companies, like Apple, NVIDIA, or Microsoft, do not seem too bothered by those provisions or indicate they are divesting out of the People's Republic of China any time soon. Ironically, they are doubling down. Apple CEO Tim Cook described China as "critical" to Apple's supply chain and has pledged to increase investment and expand research and development facilities in the region.[23]

In Europe, the GDPR has been in effect since 2018. There is no sign of those companies leaving the E.U. in droves or at all.[24] Some Big Tech companies have even praised the GDPR by saying "we should celebrate the transformative work of the European institutions tasked with the successful implementation of the GDPR" and have called for the U.S. to implement elements of it.[25]

The same is true with respect to state laws. Even with Texas's privacy law, Apple, Oracle, Softbank, OpenAI, and MGX have all pledged to increase investment into the state.[26]

All this to say, privacy laws are not a deterrent to investment.

Thus, there appears to be no correlation between a tech companies' divestment due to the enactment of comprehensive privacy laws. Any contention to the contrary is hokum.

---

[23] Dewardric W. McNeal, *Op-ed: Why An All-Smiles Chian Visit From Apple's Tim Cook Isn't Good Business*, CNBC (Mar 27, 2024), https://www.cnbc.com/2024/03/27/the-china-tour-is-a-failing-playbook-for-apple-tim-cook-and-every-ceo.html#:~:text=Tim%20Cook's%20narrative%20of%20China,Beijing%20on%20March%2024%2C%202024.

[24] Ronan Murphy, *Europe Fines US Tech: What Does it Mean?*, Center of European Policy Analysis (Apr. 23, 2025), https://cepa.org/article/europe-fines-us-tech-what-does-it-mean/; *see also* Foo Yun Chee, *Exclusive: Google to be Hit with EU Charges of Breaching Big Tech Rules, Sources Say*, Reuters (Feb. 21, 2025), https://www.reuters.com/technology/google-faces-eu-charges-breaching-dma-rules-sources-say-2025-02-21/.

[25] *E.g.*, Keynote address from Tim Cook, CEO, Apple, Inc at the 40th International Conference of EU Data Protection and Privacy Commissioners, YouTube (Oct. 18, 2018), https://www.youtube.com/watch?v=kVhOLkIs20A&t=509s.

[26] Ben Sherry, *Why Are Tech Titans Investing in Texas?*, Inc. (Feb. 25, 2025), https://www.inc.com/ben-sherry/why-are-tech-titans-investing-in-texas/91152123.

A P P E N D I X

The following submissions are available at:

https://www.govinfo.gov/content/pkg/CHRG-119shrg61893/pdf/CHRG-119shrg61893-add1.pdf

Submitted by Chair Blackburn:

Submitted by Senator Schiff: