

PROMOTING U.S. INNOVATION AND INDIVIDUAL
LIBERTY THROUGH A NATIONAL STANDARD
FOR DATA PRIVACY

HEARING
BEFORE THE
SUBCOMMITTEE ON INNOVATION, DATA, AND
COMMERCE
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS
FIRST SESSION

MARCH 1, 2023

Serial No. 118–11



Published for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

53–285 PDF

WASHINGTON : 2023

COMMITTEE ON ENERGY AND COMMERCE

CATHY McMORRIS RODGERS, Washington

Chair

MICHAEL C. BURGESS, Texas	FRANK PALLONE, JR., New Jersey
ROBERT E. LATTA, Ohio	<i>Ranking Member</i>
BRETT GUTHRIE, Kentucky	ANNA G. ESHOO, California
H. MORGAN GRIFFITH, Virginia	DIANA DeGETTE, Colorado
GUS M. BILIRAKIS, Florida	JAN SCHAKOWSKY, Illinois
BILL JOHNSON, Ohio	DORIS O. MATSUI, California
LARRY BUCSHON, Indiana	KATHY CASTOR, Florida
RICHARD HUDSON, North Carolina	JOHN P. SARBANES, Maryland
TIM WALBERG, Michigan	PAUL TONKO, New York
EARL L. "BUDDY" CARTER, Georgia	YVETTE D. CLARKE, New York
JEFF DUNCAN, South Carolina	TONY CARDENAS, California
GARY J. PALMER, Alabama	RAUL RUIZ, California
NEAL P. DUNN, Florida	SCOTT H. PETERS, California
JOHN R. CURTIS, Utah	DEBBIE DINGELL, Michigan
DEBBIE LESKO, Arizona	MARC A. VEASEY, Texas
GREG PENCE, Indiana	ANN M. KUSTER, New Hampshire
DAN CRENSHAW, Texas	ROBIN L. KELLY, Illinois
JOHN JOYCE, Pennsylvania	NANETTE DIAZ BARRAGAN, California
KELLY ARMSTRONG, North Dakota, <i>Vice</i>	LISA BLUNT ROCHESTER, Delaware
<i>Chair</i>	DARREN SOTO, Florida
RANDY K. WEBER, SR., TEXAS	ANGIE CRAIG, Minnesota
RICK W. ALLEN, Georgia	KIM SCHRIER, Washington
TROY BALDERSON, Ohio	LORI TRAHAN, Massachusetts
RUSS FULCHER, Idaho	LIZZIE FLETCHER, Texas
AUGUST PFLUGER, Texas	
DIANA HARSHBARGER, Tennessee	
MARIANNETTE MILLER-MEEKS, Iowa	
KAT CAMMACK, Florida	
JAY OBERNOLTE, California	

PROFESSIONAL STAFF

NATE HODSON, *Staff Director*
SARAH BURKE, *Deputy Staff Director*
TIFFANY GUARASCIO, *Minority Staff Director*

SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE

GUS M. BILIRAKIS, Florida

Chairman

LARRY BUCSHON, Indiana
TIM WALBERG, Michigan, *Vice Chair*

JEFF DUNCAN, South Carolina

NEAL P. DUNN, Florida

DEBBIE LESKO, Arizona

GREG PENCE, Indiana

KELLY ARMSTRONG, North Dakota

RICK W. ALLEN, Georgia

RUSS FULCHER, Idaho

DIANA HARSHBARGER, Tennessee

KAT CAMMACK, Florida

CATHY McMORRIS RODGERS, Washington

(ex officio)

JAN SCHAKOWSKY, Illinois

Ranking Member

KATHY CASTOR, Florida

DEBBIE DINGELL, Michigan

ROBIN L. KELLY, Illinois

LISA BLUNT ROCHESTER, Delaware

DARREN SOTO, Florida

LORI TRAHAN, Massachusetts

YVETTE D. CLARKE, New York

FRANK PALLONE, Jr., New Jersey *(ex*

officio)

C O N T E N T S

	Page
Hon. Gus M. Bilirakis, a Representative in Congress from the State of Florida, opening statement	2
Prepared statement	4
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement	6
Prepared statement	7
Hon. Cathy McMorris Rodgers, a Representative in Congress from the State of Washington, opening statement	8
Prepared statement	10
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	12
Prepared statement	14

WITNESSES

Graham Mudd, Founder and Chief Product Officer, Anonym	16
Prepared statement	19
Answers to submitted questions	155
Alexandra Reeve Givens, President and Chief Executive Officer, Center for Democracy & Technology	28
Prepared statement	30
Answers to submitted questions	158
Jessica Rich, Of Counsel and Senior Policy Advisor for Consumer Protection, Kelley Drye & Warren, LLP	44
Prepared statement	46
Answers to submitted questions	161

SUBMITTED MATERIAL

<i>Inclusion of the following was approved by unanimous consent.</i>	
Letter of February 28, 2023, from Eduardo F. Palacio, President, Institute of Electrical and Electronics Engineers USA, to Mrs. Rodgers, et al.	96
Letter of February 27, 2023, from Howard Fienberg, Senior Vice President, Advocacy, Insights Association, to Mr. Bilirakis and Ms. Schakowsky.	102
Letter of March 1, 2023, from Privacy for America to Mrs. Rodgers, et al.	104
Letter of February 28, 2023, from Carl Holshouser, Senior Vice President, TechNet, to Mrs. Rodgers and Mr. Pallone.	107
Letter of February 28, 2023, from Brett Meeks, Executive Director, Health Innovation Alliance, to Mrs. Rodgers and Mr. Pallone.	109
Letter of March 1, 2023, from Jim Nussle, President and Chief Executive Officer, Credit Union National Association, to Mr. Bilirakis and Ms. Schakowsky.	110
Letter of February 28, 2023, from Engine to Subcommittee on Innovation, Data, and Commerce members.	112
Letter of February 28, 2023, from Tina O. Grande, Chair, Confidentiality Coalition, and Executive Vice President, Policy, Healthcare Leadership Council, to Mr. Bilirakis and Ms. Schakowsky.	115
Letter of February 28, 2023, from Brad Thaler, Vice President of Legislative Affairs, National Association of Federally-Insured Credit Unions, to Mr. Bilirakis and Ms. Schakowsky.	117

VI

	Page
Letter of Feb. 26, 2023, from Brandon Pugh, Policy Director and Senior Fellow, Cybersecurity & Emerging Threats Team, R Street, to Mr. Bilirakis. ¹	
Letter of February 27, 2023, from Sharon Wilson G�no, President, National Multifamily Housing Council, and Robert Pinnegar, President and Chief Executive Officer, National Apartment Association, to Mr. Bilirakis and Ms. Schakowsky.	120
Letter of February 28, 2023, from Main Street Privacy Coalition to Mrs. Rodgers, et al.	123
Letter of March 1, 2023, from Jeff Patchen, Director of Government Affairs, Electronic Transactions Association, to Mr. Bilirakis and Ms. Schakowsky. .	127
Letter of March 1, 2023, from Craig Albright, Vice President, U.S. Government Relations, BSA–The Software Alliance, to Mr. Bilirakis and Ms. Schakowsky.	129
Letter of March 1, 2023, from Peter A. Feldman, Commissioner, Consumer Product Safety Commission, to Mr. Bilirakis and Ms. Schakowsky.	132
Statement of Morgan Reed, President of ACT–The App Association and Connected Health Initiative.	134
Letter of March 1, 2023, from Jordan Crenshaw, Vice President, Chamber Technology Engagement Center, U.S. Chamber of Commerce, to Mr. Bilirakis and Ms. Schakowsky.	140
Report of the Information Technology and Innovation Foundation, “The Looming Cost of a Patchwork of State Privacy Laws,” January 2022. ²	
Letter of March 1, 2023, from Robyn M. Boerstling, Vice President, Infrastructure, Innovation and Human Resources Policy, National Association of Manufacturers, to Mr. Bilirakis and Ms. Schakowsky.	146
Letter of February 28, 2023, from Jesselyn McCurdy, Executive Vice President of Government Affairs, Leadership Conference on Civil and Human Rights, to Mrs. Rodgers, et al.	148
Letter of September 26, 2022, from the Association of State Criminal Investigative Agencies, et al., to Hon. Nancy Pelosi, et al.	151
Letter of September 26, 2022, from Patrick Yoes, National President, Fraternal Order of Police, and Chief Dwight Henninger, President, International Association of Chiefs of Police, to Hon. Nancy Pelosi, et al.	153

¹The letter has been retained in committee files and is available at <https://docs.house.gov/meetings/IF/IF17/20230301/115376/HHRG-118-IF17-20230301-SD033.pdf>.

²The report has been retained in committee files and is available at <https://docs.house.gov/meetings/IF/IF17/20230301/115376/HHRG-118-IF17-20230301-SD021.pdf>.

PROMOTING U.S. INNOVATION AND INDIVIDUAL LIBERTY THROUGH A NATIONAL STANDARD FOR DATA PRIVACY

WEDNESDAY, MARCH 1, 2023

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 8:33 a.m., in the John D. Dingell Room 2123, Rayburn House Office Building, Hon. Gus M. Bilirakis (chairman of the subcommittee) presiding.

Members present: Representatives Bilirakis, Bucshon, Walberg, Duncan, Dunn, Lesko, Pence, Armstrong, Allen, Fulcher, Harshbarger, Cammack, Rodgers (ex officio), Schakowsky (subcommittee ranking member), Castor, Dingell, Kelly, Soto, Trahan, Clarke, and Pallone (ex officio).

Also present: Representatives Carter and Obernolte.

Staff present: Sarah Burke, Deputy Staff Director; Michael Cameron, Professional Staff Member, Innovation, Data, and Commerce; Jessica Herron, Clerk, Innovation, Data, and Commerce; Nate Hodson, Staff Director; Tara Hupman, Chief Counsel; Peter Kielty, General Counsel; Emily King, Member Services Director; Tim Kurth, Chief Counsel, Innovation, Data, and Commerce; Brannon Rains, Professional Staff Member, Innovation, Data, and Commerce; Lacey Strahm, Fellow, Innovation, Data, and Commerce; Michael Taggart, Policy Director; Teddy Tanzer, Senior Counsel, Innovation, Data, and Commerce; Hannah Anton, Minority Staff Assistant; Ian Barlow, Minority FTC Detailee; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Daniel Greene, Minority Professional Staff Member; Tiffany Guarascio, Minority Staff Director; Perry Hamilton, Minority Member Services and Outreach Manager; Lisa Hone, Minority Chief Counsel, Innovation, Data, and Commerce; Mackenzie Kuhl, Minority Digital Manager; Joe Orlando, Minority Senior Policy Analyst; Greg Pugh, Minority Staff Assistant; and Andrew Souvall, Minority Director of Communications, Outreach, and Member Services.

Mr. BILIRAKIS. Good morning. The Subcommittee on Innovation, Data, and Commerce will come to order.

The Chair recognizes himself for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. GUS M. BILIRAKIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Good morning, again. I appreciate y'all being here. We got an early jump start on the day to accommodate our friends across the aisle, who have a issues conference later this afternoon. So I am confident we will make the most of our time this morning.

We made great strides last Congress, as you know, with the leadership of this committee, demonstrating that we can come together in a bipartisan fashion for the American people. I look forward to continuing and completing that important work this Congress.

Earlier this week, the House passed H.R. 538, the Informing Consumers about Smart Devices Act, from Representatives Curtis and Moulton, with broad bipartisan support. I want to recognize Chair Cantwell and Ranking Member Cruz in the Senate for sponsoring the Senate companion bill, which I take as a strong sign that the Senate cares about American's privacy. I hope I am right. I thank these Members for working on legislation that complements this committee's broader privacy goals and provides great transparency to Americans about the ability for devices to secretly record them.

This is just one of many examples of why congressional action on broader comprehensive privacy and data security is desperately needed and why we are holding this hearing today, the second in a series of three.

With that, I want to express my gratitude to our panelists for being here. We appreciate you very much, not only for bearing with us with the early start time but also for sharing your expertise today. Each of you bring important insights that will help our committee advance comprehensive privacy and data security legislation this Congress.

Americans need and deserve more transparency over how their information is collected, processed, and transferred. In the past several years, our constituents have likely noticed the internet becoming more personalized for them, whether they are seeing more targeted advertisements, showing items that they recently viewed on another website, or experiencing content on social media that matches what they have interacted with elsewhere. Sometimes it is scary stuff.

To some, these practices may be viewed as more convenient for their shopping or useful for how they digest information. But others may find this practice is invasive and unsolicited. So let's give Americans the right to choose if they want this or not. Why not?

Mr. Mudd, thank you, again, for being here to walk us through how legislation can work for businesses operating in the digital ecosystem and to share your expertise about how we can both protect innovation in our economy and still give Americans freedom to choose what to do with their personal and sensitive data. I know we can get this done. I appreciate you being here, sir.

We also need to ensure legislation works for everyone and doesn't adversely impact our constituents or impede on the basic liberties that every American deserves.

Ms. Givens, I want to thank you for your expertise on these matters, as well as for your support over the last year in advancing comprehensive legislation. Thank you so much.

Lastly, we need to ensure responsible government approach to enforcing clear rules for businesses to comply. Companies, especially small startups, shouldn't be subject to random or punitive letters in the mail notifying them that certain practices could be unfair or deceptive. It is essential that the FTC enforce the laws so that we as a Congress enact and, specifically, authorize but not go rogue beyond the rules of the road we provide. This type of regulatory certainty is needed for businesses to comply. They must comply, but, again, it has got to be fair.

Ms. Rich, thank you for testifying today again. You have great insights regarding the role of the FTC in enforcing laws but doing so in a way that doesn't unduly burden legitimate business activity. I look forward to continuing to work with you on achieving the right balance for the FTC to enforce a national privacy and data security law to protect Americans of all ages while at the same time ensure that businesses that follow the rules aren't subject to government overreach and frivolous litigation. The committee appreciates your deep institutional knowledge and insight. Thank you so much.

Again, thanks again to our panel for being here, and I look forward to your testimony.

[The prepared statement of Mr. Bilirakis follows:]

**Opening Statement of Chair Gus Bilirakis
As Prepared for Delivery
Committee On Energy and Commerce
Subcommittee on Innovation, Data, and Commerce
Hearing entitled “Promoting U.S. Innovation and Individual Liberty through
a National Standard for Data Privacy”
March 1, 2023**

Good morning everyone. We got an early jump start on the day to accommodate our friends across the aisle who have a retreat later today. I’m confident we’ll make the most of our time this morning.

We made great strides last Congress with the leadership of this Committee demonstrating that we can come together in a bipartisan fashion for the American people. I look forward to continuing and completing that important work this Congress.

Earlier this week, the House passed H.R. 538, the Informing Consumers about Smart Devices Act from Representatives Curtis and Moulton, with broad bipartisan support. I want to recognize Chair Cantwell and Ranking Member Cruz in the Senate for sponsoring the Senate Companion bill, which I take as a strong sign that the Senate cares about Americans’ privacy. I thank these Members for working on legislation that compliments this Committee’s broader privacy goals and provides greater transparency to Americans about the ability for devices to secretly record them. This is just one of many examples why Congressional action on broader comprehensive privacy and data security is desperately needed and why we are holding this hearing today, the second in a series of three.

With that I want to express my gratitude to our panelists not only for bearing with us for the early start time, but also for sharing your expertise today. Each of you bring important insights that will help our Committee advance comprehensive privacy and data security legislation this Congress.

Americans need and deserve more transparency over how their information is collected, processed, and transferred. In the past several years, our constituents have likely noticed the internet becoming more personalized for them – whether they are seeing more targeted advertisements showing items that they’ve recently viewed on another website, or experiencing content on social media that matches what they’ve interacted with elsewhere. To some, these practices may be viewed as more convenient for their shopping or useful for how they digest information. But others may find this practice invasive and unsolicited. So let’s give Americans the right to choose if they want this or not.

Mr. Mudd, thank you for being here to walk us through how legislation can work for businesses operating in the digital ecosystem and to share your expertise about how we can both protect innovation in our economy and still give Americans freedoms to choose what to do with their personal and sensitive data.

We also need to ensure legislation works for everyone and doesn’t adversely impact our constituents or impede on the basic liberties that every American deserves. Miss Givens, I want

to thank you for your expertise on these matters, as well as for your support over the last year in advancing comprehensive legislation.

Lastly, we need to ensure responsible government approach to enforcing clear rules for businesses to comply. Companies, especially small startups, shouldn't be subject to random or punitive letters in the mail notifying them that certain practices could be unfair or deceptive. It is essential that the FTC enforce the laws that we as a Congress enact and specifically authorize, but not go rogue beyond the rules of the road we provide. This type of regulatory certainty is needed for businesses to come into compliance.

Miss Rich, thank you for testifying. You have great insights regarding the role of the FTC in enforcing laws but doing so in a way that doesn't unduly burden legitimate business activity. I look forward to continuing to work with you on achieving the right balance for the FTC to enforce a national privacy and data security law to protect Americans of all ages, while at the same time ensure that businesses that follow the rules aren't subject to government overreach and frivolous litigation. The Committee appreciates your deep institutional knowledge and insight.

Thank you again to our panel for being here and I look forward to your testimony.

Mr. BILIRAKIS. The Chair now recognizes the subcommittee ranking member, Ms. Schakowsky, for her 5 minutes for an opening statement. Good morning.

OPENING STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Good morning, everyone. Thank you so much, Mr. Chairman.

And I really want to begin by saying how proud I am of the work that this subcommittee has done really over the years, particularly in the last session of Congress, in a bipartisan way. And I am really looking forward, as you said in your beginning remarks, that we can do this together, that we can go forward.

We were almost there. We were able to pass in a unanimous way, almost, the American Data Privacy and Protection Act, again, working together.

We heard the cry of the vast majority of Americans who are really tired of feeling helpless online. We heard from stakeholders from every corner of government and civic society—civil society—and industry at six different roundtables that we had. But absent any action by the—by the Congress, Big Tech is collecting ever more information about us, our personal information, intimate data. And these companies know our habits, they know our finances, where we are, where we live, where we are going. And when you browse the web or wear a smartwatch, a tech company is tracking you.

So they use this data to manipulate us, to addict us, and to keep us on their platforms so that they can provide even more ads to us, or they sell the data to the highest bidder so that companies that you don't even know what their names are or who they are can build a profile about you.

Harmful targeting of advertising on social media has exacerbated the mental health problems that we face, particularly among our young people. Our adolescents, our kids are the most vulnerable. Our teenagers, we have to make sure that we are protecting them.

All this is in the name of profit. It is time—it is time, and the time has really passed, I think, for us to do a data privacy law, and I really, really look forward to working together. Our past effort I think provides, once again, the guidelines for how we can move together, and I absolutely look forward to building on the momentous gains that we have made.

And so I think it is time for us to roll up our sleeves in a bipartisan way to get to work. The United States is far behind, and we need to catch up with States that are beginning to introduce their own privacy laws, many different ones from around the country, and to give consumers what they want.

And, with that, I yield back.

[The prepared statement of Ms. Schakowsky follows:]

Committee on Energy and Commerce**Opening Statement as Prepared for Delivery
of****Subcommittee on Innovation, Data, and Commerce Ranking Member Jan Schakowsky*****Hearing on “Promoting U.S. Innovation and Individual Liberty Through a National Standard
for Data Privacy.”*****March 1, 2023**

We made it almost to the finish line on data privacy by working together. A majority of Americans agree: consumers need comprehensive federal data privacy protections.¹

That’s because the internet is not living up to its promise. The early internet promised more social connections, new communities, and more innovation and economic opportunity. But these benefits have come at the expense of our privacy.

Big Tech has become dependent on collecting ever more personal and intimate data about us. Data on our habits, our finances, who we love, where we live, and our most sensitive health data. Every time you browse the web or wear a smart watch, a tech company is tracking you. They use this data to manipulate us, to addict us, and to keep us on their platforms so we can be fed more ads. Or they sell the data to the highest bidder so that companies you’ve never heard of can build profiles of you. Social media has become like cigarettes, addicting in the name of profit.

Like with cigarettes, our teenagers are particularly affected. Harmful targeted advertising on social media has exacerbated the mental health crisis plaguing our young people. Americans are tired of feeling helpless online. It is time to pass data privacy legislation that protects consumers and promotes innovation.

I’d like to acknowledge, with immense gratitude, the years of tireless work on both sides of the aisle. Our efforts prove, once again, that privacy is not a partisan or an extreme issue. The “American Data Privacy and Protection Act” represented a groundbreaking milestone and is inspiring privacy advocates across the country. Just last summer, it overwhelmingly passed the Energy & Commerce Committee 53-2.

I look forward to today’s bipartisan hearing to build on our momentum, years in the making, to pass transformational privacy protections for all Americans. It’s time to return control of their data back to the American people, and to finish what we started last year.

¹ <https://iapp.org/news/a/poll-55-of-registered-us-voters-want-federal-privacy-law/>

Mr. BILIRAKIS. I thank the ranking member.

The Chair now recognizes the chair of the full committee, Mrs. Rodgers, for 5 minutes for her opening statement.

**OPENING STATEMENT OF HON. CATHY McMORRIS RODGERS,
A REPRESENTATIVE IN CONGRESS FROM THE STATE OF
WASHINGTON**

Mrs. RODGERS. Good morning. Thank you to the witnesses for being here this morning. Really appreciate this panel. Your testimony is essential as we keep the momentum going, as Ms. Schakowsky was just mentioning, for a strong data privacy and security and those protections for all Americans.

This subcommittee's first hearing this year focused on data privacy and security to ensure America's global competitive edge against China. Today's second hearing in our series will consider what a strong national data privacy standard will mean in our everyday lives to rein in Big Tech, protect kids online, and put people in charge of their data. These discussions build on the bipartisan, bicameral ADPPA, which moved through this committee last year with a vote of 53 to 2. That was the first time this committee reached such a milestone, and no other committee has come close on a national privacy and data security standard with bipartisan support necessary to clear the House and make the Senate take notice.

This is a new Congress with new considerations, so we must continue to improve on the legislation from last Congress, build consensus among stakeholders. Bringing together experience in business, civil society, and government is the three-legged stool that will support our efforts in developing bipartisan, comprehensive privacy and data security legislation. We must continue our work so individuals can exercise their rights, businesses can continue to innovate, and the Government's role is clearly defined.

Today turns that conversation inward so we are preserving the engine of innovation while ensuring that we aren't just dollar signs for data brokers and Big Tech. They are harvesting people's data, selling or sharing it without their knowledge, and not keeping it secure. We need a national data privacy standard that changes the status quo regarding people's data.

Right now, there are no robust protections. Americans have no say over whether and where their personal data is sold and shared. They have no guaranteed way to access, delete, or correct their data. And they have no ability to stop the unchecked collection of their sensitive personal information. This isn't acceptable.

Data brokers' and Big Tech's day of operating in the dark should be over. People should trust their data is being protected.

We are at an inflection point to ensure our personal information is responsibly collected so artificial intelligence is developed with our values. We need to ensure that the metaverse doesn't become the next frontier of exploitation for our kids. That requires a broad, comprehensive bill that will address all Americans' data and put even stronger guardrails around our kids. That is why the American Data Privacy and Protection Act included the strongest internet protections for children of any legislation last Congress. And its

protections did not stop with kids. ADPPA gave everyone data protections no matter where they live and no matter their age.

We will continue to build on ADPPA this Congress and get these strong protections for our kids and all Americans signed into law.

I want to thank the ranking member, Ranking Member Pallone, other colleagues, ranking member of this subcommittee, Jan Schakowsky, as well as the chairman of this subcommittee, Gus Bilirakis, and colleagues on this committee across the aisle for working together on this legislation. We have a shared goal here, and we are going to continue this work, and we are going to get it done in this Congress.

I look forward to today's hearing and for our privacy series to continue on March 23, when TikTok's CEO is before this committee.

Thank you, and I yield back.

[The prepared statement of Mrs. Rodgers follows:]

**Opening Statement of Chair Cathy McMorris Rodgers
As Prepared for Delivery
Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce
Hearing entitled “Promoting U.S. Innovation and Individual Liberty through
a National Standard for Data Privacy”
March 1, 2023**

Good morning.

Thank you to our panel of witnesses here this morning.

Your testimony today is essential, as we keep the momentum going for strong data privacy and security protections for all Americans.

This subcommittee’s first hearing this year focused on data privacy and security to ensure America’s global competitive edge against China.

Today’s second hearing in our series will consider what a strong national data privacy standard will mean in our everyday lives to rein in Big Tech, protect kids online, and put people in charge of their data.

These discussions build on the bipartisan, bicameral ADPPA, which we moved through the committee last year with a vote of 53-2.

That was the first time this committee reached such a milestone, and no other committee has come close on a national privacy and data security standard with the bipartisan support necessary to clear the House and make the Senate take notice.

This is a new Congress, with new considerations, so we must continue to improve on the legislation from last Congress and build consensus amongst stakeholders.

Bringing together experience in business.... civil society.... and government.... is the three-legged stool that will support our efforts in developing bipartisan comprehensive privacy and data security legislation.

We must continue our work so that individuals can exercise their rights.... businesses can continue to innovate.... and the government’s role is clearly defined.

Today turns that conversation inward so we are preserving the engine of innovation while ensuring that we aren’t just dollar signs for data brokers and Big Tech.

They are harvesting people’s data, selling or sharing it without their knowledge, and not keeping it secure.

We need a national data privacy standard that changes the status quo regarding people's data.

Right now, there are no robust protections.

Americans have no say over whether and where their personal data is sold and shared...

... they have no guaranteed way to access, delete, or correct their data...

... and they have no ability to stop the unchecked collection of their sensitive personal information.

This isn't acceptable. Data brokers' and Big Tech's days of operating in the dark should be over.

People should trust their data is being protected.

We are at an inflection point to ensure our personal information is responsibly collected so artificial intelligence is developed with our values.

We need to ensure that the metaverse doesn't become the next frontier of exploitation for our kids.

That requires a broad comprehensive bill that will address all Americans' data, and puts even stronger guardrails around our kids.

That's why the American Data Privacy and Protection Act includes the strongest internet protections for children of any legislation last Congress.

And its protections does not stop with kids.

ADPPA gives everyone data protections—no matter where they live and no matter their age.

We will continue to build on ADPPA this Congress and get these strong protections for kids and all Americans signed into law.

Thank you, Ranking Member Pallone and my colleagues across the aisle, for continuing to work with us.

We share the goal for strong bipartisan consensus like we had last year on ADPPA.

I look forward to today's hearing... and for our privacy series to continue on March 23rd when Tik Tok's CEO is before the Committee.

Thank you, I yield back.

Mr. BILIRAKIS. Thank you. I want to thank the chair. And again, as you said, we got to get it across the finish line this time, but we did our job last Congress under your leadership, Madam Chair, and the leadership of the ranking member. So we can make a good bill even better. So we appreciate that very much.

With that, the Chair recognizes the ranking member of the full committee, my friend, Mr. Pallone, for his 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Chairman Bilirakis.

Last Congress, when I chaired the committee, I was proud to work with then-Ranking Member Rodgers and now Chair Rodgers and the other subcommittee leaders on the American Data Privacy and Protection Act. And that was the first bipartisan and bicameral comprehensive data privacy legislation in decades. And this was a historic achievement with a 53 to 2 vote out of committee.

In this subcommittee's first hearing of this Congress, I was pleased, but not surprised, to hear Chair Rodgers reaffirm her commitment to advancing this bill.

Simply put, as we will hear from today's witnesses, we need comprehensive Federal data privacy legislation, and we need it urgently. Today, many of our essential consumer products, especially those offered by the largest tech companies, require consumers, including children and teens, to trade their personal data for services. And this is not a real choice. People can't thrive in our digital economy without access to websites, mobile applications, email services, and other forms of online communication.

Members of both parties talk a lot about holding Big Tech accountable, and I firmly believe that the way to do that is by adopting a strong national privacy standard that limits the excesses of Big Tech and makes the digital world safer.

The testimony we will hear today will illustrate the fact that the lack of a national privacy standard doesn't just hurt consumers, it also hurts small and emerging businesses by favoring big providers at the expense of new competitors. Providing certainty to all consumers, businesses, and markets about fair and appropriate data collection and use is crucial for continued American innovation. We simply cannot go another Congress without passing comprehensive privacy legislation.

Our legislation last Congress includes input from many of you on this subcommittee and countless other stakeholders. It directly confronts and reaches important compromises on the sticking points which derailed earlier congressional efforts. The American Data Privacy and Protection Act will put people back in control of their personal data, stop data collection abuses by Big Tech, provide important protections for kids, rein in the shadowy world of data brokers, and establish strong Federal data security standards.

The legislation achieves all this by starting with the fundamental shift in how data is collected, used, and transferred. It rejects the coercive notice and consent system that has failed to protect Americans' data privacy and security. Instead, the bill adopts a data

minimization obligation. It requires companies to limit the personal information they collect. They will only be able to collect what is reasonably necessary and proportionate to providing the services that consumers are requesting.

At this subcommittee's first hearing this year, we heard testimony that data minimization protects consumer privacy and is critical for cybersecurity and national security, and that is exactly what our bill did. And again, the American Data Privacy and Protection Act also protects kids from Big Tech. It bans targeted advertising to children under 17, and covered entities will not be able to transfer covered data belonging to children without consent. To help enforce these protections for kids, the bill establishes a youth privacy and marketing division at the Federal Trade Commission.

Our legislation also shines a light on the shadowed world of data brokers that profit from buying and selling our personal data. These companies don't interact with consumers directly, but they do collect and sell massive amounts of consumer data, including sensitive personal data like health information and precise geolocation data that identifies a consumer's location within 18 feet. We must stop these data brokers from collecting, using, and selling consumers' data without their knowledge or permission.

The American Data Privacy and Protection Act will require data brokers to register with the FTC and will provide consumers with a single mechanism to opt out of data collection by all registered brokers.

Now, while Congress has stalled on privacy for years, the rest of the world has not, ceding American leadership on technological regulation. The European Union has passed comprehensive privacy laws, and this bill would immediately reset the global landscape.

So I want to thank the witnesses for being here today to shed even more light on the need for a national privacy standard. I want to thank Chairwoman Rodgers, Ranking Member Schakowsky, Chairman Bilirakis, and the members of this subcommittee for their really tireless efforts and their unwavering commitment to move a comprehensive data privacy bill across the finish line this Congress. I know that we can do it. So thank you again.

I yield back to the chairman.

[The prepared statement of Mr. Pallone follows:]

Committee on Energy and Commerce

**Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.**

Innovation, Data, and Commerce Subcommittee Hearing on “Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy.”

March 1, 2023

Last Congress, when I Chaired this Committee, I was proud to work with then-Ranking Member Rodgers and this Subcommittee’s leaders on the American Data Privacy and Protection Act (ADPPA) - the first bipartisan and bicameral comprehensive data privacy legislation in decades. This was a historic achievement, with a 53-2 vote out of Committee. In this Subcommittee’s first hearing of this Congress, I was pleased, but not surprised, to hear Chair Rodgers reaffirm her commitment to advancing that bill.

Simply put, as we will hear from today’s witnesses, we need comprehensive, federal data privacy legislation. And we need it urgently.

Today, many of our essential consumer products—especially those offered by the largest technology companies—require consumers, including children and teens, to trade their personal data for services. This is not a real choice. People cannot thrive in our digital economy without access to websites, mobile applications, email services, and other forms of online communication.

Members of both parties talk a lot about holding big tech accountable. I firmly believe that the way to do that is by adopting a strong national privacy standard that limits the excesses of Big Tech and makes the digital world safer.

The testimony we will hear today will illustrate the fact that the lack of a national privacy standard doesn’t just hurt consumers. It also hurts small and emerging businesses by favoring big providers at the expense of new competitors. Providing certainty to all consumers, businesses, and markets about fair and appropriate data collection and use is crucial for continued American innovation.

We simply cannot go another Congress without passing comprehensive privacy legislation. Our legislation last Congress includes input from many of you on this Subcommittee and countless other stakeholders. It directly confronts—and reaches important compromises—on the sticking points which derailed earlier Congressional efforts.

The American Data Privacy and Protection Act will put people back in control of their personal data, stop data collection abuses by Big Tech, provide important protections for kids, rein in the shadowy world of data brokers, and establish strong federal data security standards.

March 1, 2023

Page 2

The legislation achieves all this by starting with a fundamental shift in how data is collected, used, and transferred. It rejects the coercive “notice and consent” system that has failed to protect Americans’ data privacy and security.

Instead, the ADPPA adopts a data minimization obligation. It requires companies to limit the personal information they collect. They will only be able to collect what is reasonably necessary and proportionate to providing the services consumers are requesting. At this Subcommittee’s first hearing this year, we heard testimony that data minimization protects consumer privacy and is critical for cybersecurity and national security, and that’s exactly what our bill did.

The American Data Privacy and Protection Act also protects kids from Big Tech. It bans targeted advertising to children under 17. And covered entities will not be able to transfer covered data belonging to children without consent. To help enforce these protections for kids, the bill establishes a Youth Privacy and Marketing Division at the Federal Trade Commission (FTC).

Our legislation also shines a light on the shadow world of data brokers that profit from buying and selling our personal data. These companies don’t interact with consumers directly, but they do collect and sell massive amounts of consumer data, including sensitive personal data like health information and precise geolocation data that identifies a consumer’s location within 18 feet.

We must stop these data brokers from collecting, using, and selling consumers’ data without their knowledge or permission. The American Data Privacy and Protection Act will require data brokers to register with the FTC and will provide consumers with a single mechanism to opt out of data collection by all registered brokers.

While Congress has stalled on privacy for years, the rest of the world has not, ceding American leadership on technological regulation. The European Union has passed comprehensive privacy laws. This bill would immediately reset the global landscape.

I want to thank the witnesses for being here today to shed even more light on the need for a national privacy standard. I thank Chair Rodgers, Ranking Member Schakowsky, Chair Bilirakis and the members of this Subcommittee for their tireless efforts and their unwavering commitment to move comprehensive data privacy legislation across the finish line this Congress.

Thank you and I yield back.

Mr. BILIRAKIS. I thank the ranking member.

We have now concluded with Member opening statements. The Chair would like to remind Members that, pursuant to the committee rules, all Members' opening statements will be made part of the record.

We would like to, again, thank all of our witnesses for being here, again, earlier than normal, to testify before the committee.

Today's witnesses will have 5 minutes to provide oral testimony, which will be followed by a round of questions from Members.

Our witness panel for today's hearing will include Mr. Graham Mudd, who is the founder and chief product officer of Anonym. I asked him yesterday if he was related to the late Roger Mudd, who was a great journalist, and he said yes, distantly. That is pretty cool. If you don't ask, you don't get the answer.

And then Ms. Alexandra Reeve Givens, who is the president and CEO of Center for Democracy and Technology.

And Ms. Jessica Rich, of counsel and senior policy advisor for consumer protection, Kelley, Drye & Warren, LLP.

So, Mr. Mudd, you are recognized for 5 minutes. We appreciate you being here again, sir.

STATEMENTS OF GRAHAM MUDD, FOUNDER AND CHIEF PRODUCT OFFICER, ANONYM; ALEXANDRA REEVE GIVENS, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CENTER FOR DEMOCRACY & TECHNOLOGY; JESSICA RICH, OF COUNSEL AND SENIOR POLICY ADVISOR FOR CONSUMER PROTECTION, KELLEY DRYE & WARREN, LLP

STATEMENT OF GRAHAM MUDD

Mr. MUDD. [Inaudible.] My apologies.

Chairman Bilirakis, Ranking Member Schakowsky, Chair Rodgers, Ranking Member Pallone, and distinguished members of this committee, thank you for the opportunity to testify at this important hearing.

My name is Graham Mudd, and I am cofounder and chief product officer of Anonym, a privacy technology company. I want to begin by thanking you for pushing forward ADPPA. I am looking forward to the passage of strong Federal privacy legislation along with strong enforcement authority.

We are here to talk about creating a more privacy-safe internet for Americans. The collection, sharing, and use of data for advertising is at the heart of the digital privacy challenge facing our country and the world. We started Anonym because we believed the notion that you can't have both privacy and an efficient digital advertising ecosystem is a false dichotomy. While we are focused on building technologies that support privacy, we are also convinced that strong Federal privacy legislation is necessary if we want to make progress on this issue.

We have been part of the development of internet advertising since the early days. We spent more than 10 years helping to develop Meta's data-driven advertising business. Over the years, consumer data has become an increasingly powerful asset. The companies we work for and competed with adopted increasingly aggres-

sive approaches in how they used data to improve their advertising products. To be frank, we helped develop these methods.

But in the past few years, we and many others have become increasingly uncomfortable with the privacy implications of the practices we helped pioneer. And so we started Anonym with a simple goal: to provide technically guaranteed privacy protections to consumers while enabling effective digital advertising.

Today, digital advertising is supported by the wholesale and unregulated sharing of individual-level data between advertisers and the companies that run ads for them. The mechanics are fairly complex, so I will just use a recent personal example.

My wife and I are doing a few renovations at our home, so I have been spending a lot of time on home improvement sites, like Home Depot. Not surprisingly, I see ads for products I researched, and some I haven't but might find interesting. Most of you and most Americans are familiar with this experience. Sometimes it is useful. Oftentimes it is a bit unsettling. So how did this come to be?

Well, the majority of companies who run digital ads, including The Home Depot, have added tracking software from dozens of ad platforms that they do business with. These trackers are from ad tech companies most of you have never heard of, in addition to large tech companies like Google and Meta, Pinterest, et cetera. Now, these trackers collect information about my browsing and buying at sites like Home Depot, and they share that data with ad platforms. This data allows platforms to effectively target ads to me, and it allows advertisers like Home Depot to measure how well those ads work so they can spend their ad dollars efficiently. But at scale, this approach allows ad platforms to build tremendously rich profiles of people's browsing and buying behavior across millions of websites.

Now, does the average American expect and appreciate that their internet behavior on millions of sites is being beamed to dozens of advertising companies so they can build a profile on them? Of course they don't. We call this the profiling problem, and we believe the profiling problem is at the heart of the privacy challenge we should all be focused on. The solution to this challenge, we believe, requires two ingredients.

First, strong Federal privacy legislation. Legislation that ensures that Americans' data is collected and, importantly, shared only in ways they would reasonably expect or with their explicit consent. Legislation that increases protection for children beyond COPPA. Legislation that unifies the current protections that exist at the State level to provide protections for all Americans. Legislation that provides for strong and clear enforcement authority. And we believe that enlightened legislation like ADPPA has all of these components.

The second critical ingredient is technology. After all, technology got us into this problem, so it stands to reason it can help get us out of it. Privacy-enhancing technologies are used in many other industries—in financial services, in pharmaceuticals, and in government—to extract value from data without compromising the privacy of individuals. A number of companies, ours included, are working to apply these technologies to make digital advertising

more private by default. These technologies can, in effect, reduce the cost of improving privacy.

So while technology can help, ultimately we have got to be clear-eyed about the incentives at play. We would all love for ad platforms and publishers to proactively adopt more privacy-preserving technologies, but doing so alone means putting oneself at a massive competitive disadvantage. A strong regulatory backstop is critical in addressing this incentive problem.

With regulation in place, I am confident that we and others will find innovative ways to leverage privacy-enhancing technologies to support business growth while guaranteeing the privacy of all Americans.

[The prepared statement of Mr. Mudd follows:]



Written Testimony of:

Graham Mudd
 Founder & Chief Product Officer
 Anonym, Inc

Hearing:

Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy
 House Subcommittee on Innovation, Data, and Commerce
 March 1, 2023, at 8:30 AM

Chairman Bilirakis, Ranking Member Schakowsky, and distinguished Members of this Committee, thank you for the opportunity to testify at this important hearing.

My name is Graham Mudd, and I am co-founder and chief product officer of Anonym, Inc., a privacy-technology company that is focused on solving the privacy challenges facing digital advertising. My colleague and fellow cofounder, Brad Smallwood, who also is here with us today, is our chief executive officer. We're here, however, not to pitch our company—although we hope to talk a bit about what we're doing in privacy tech—but to show our support for reintroduction of the bicameral, bipartisan American Data Privacy Protection Act (ADPPA), which we believe would create a comprehensive privacy framework that would benefit all American consumers.

So, I want to begin by thanking you all—and particularly Chair Rodgers and Ranking Member Pallone of the Energy and Commerce Committee for their groundbreaking work in the last Congress—for introducing this comprehensive framework designed to set higher standards for protecting American data privacy. We at Anonym share your belief that the ADPPA has the potential to mark a historical watershed in privacy law and policy. This legislation, we believe, will reform data-privacy practices – and at the same time it will promote the ethical use of data that supports the evolution of stronger digital services.

My co-founder and I have been part of the development of the internet advertising ecosystem since the first wave of the internet in the late 1990s. Prior to Anonym, we both worked at Meta for more than 10 years, where we helped build and run the advertising business. We ran teams responsible for building the products that marketers leveraged to deliver and measure their advertising. Prior to that, we worked in product and analytics roles at Yahoo and other firms.

In all of our roles over the past 25-plus years, consumer behavioral data was an incredibly powerful asset in building more relevant products for people and more effective advertising solutions for businesses. As a result, acquiring data and putting it to use in increasingly sophisticated ways was always a strategic imperative. However, over the years, a tension began to emerge – the development of the rich consumer profiles that were so powerful in improving products of all kinds came at the cost of individuals' privacy. This trade-off is why we're here today.

We started Anonym with a simple goal – to provide technical privacy protections to consumers while at the same time ensuring that businesses continue to have the tools they need to grow. In effect, our goal is to reduce the trade-off cost of becoming a more privacy-safe digital ecosystem.

But technical protections alone are not sufficient. That's because without regulation and strong enforcement there is little incentive for companies to stop leveraging individuals' data to enhance their business.

How Did We Get Here?

To chart a path forward, it's often useful to reflect on what led to the status quo. Media companies have always strived to put the right information in front of their consumers. This competition for relevance – whether focused on content or advertising – has benefited consumers tremendously. Until the explosion of the internet at the turn of the century, almost all media were broadcast. Producers and

editors curated content to ensure that it was relevant to the audience they were serving. Advertisers used audience research to understand the demographic makeup of these audiences so they could place their ads where their target customers were likely to see them.

Digital advertising initially relied on the same approach. Advertisers used audience research to understand the demographics of the visitors to web sites or sections of sites, like Yahoo Sports. Just as with TV, radio and print, advertisers ran ad campaigns based on informed generalizations. There were of course exceptions, like direct mail, which has always harnessed individual-level data. In fact, political campaigns were among the earliest users of detailed data for content and advertising delivery.

But then internet search changed everything. Search-based advertising for the first time allowed companies to segment their audience at scale efficiently, and importantly, match the advertising to a consumer's interests and behaviors. The opportunity to use the information about what a consumer searched for to target advertising was game changing to advertisers, consumers, and search providers alike.

Other digital publishers and ad platforms that served display advertising (e.g. banner ads) weren't as naturally blessed with the rich consumer data search providers had. To compensate, display platforms sought ways to generate and aggregate consumer data from as many sources as possible and build rich consumer profiles with it. Ad networks collected browsing and ad-click data from tens of thousands of publishers. Data brokers, who had previously focused on direct mail, began selling data to digital display-ad platforms. Finally, social media companies began accumulating vast user bases – and since their users were required to log in, building rich profiles was much easier, given their access to highly accurate consumer identity data. To further extend their ability to collect, measure, and improve ad performance, many major ad platforms began using “pixels” to collect data from across the web.

A Pixel is Worth a Thousand Words

Pixels, and their mobile-app equivalent, [tracking SDKs](#), are an elegantly simple yet massively powerful set of technologies, so they're important to understand. At the most basic level, pixels are small pieces of code that look for a "cookie" to identify a device or user. They are deployed by a specific ad platform to many websites and apps that they don't own or control. When a person visits a website with a pixel installed, the pixel sends data about the user's behavior on that website back to the ad platform, where it is then typically associated with that user's profile.

I'll share a recent personal example to make this all a bit more concrete. My wife and I are in the process of completing a few home renovations. As a result, I've spent a fair bit of time on home improvement sites like Home Depot. For the past few weeks, I've seen ads across the web for products I've researched (and sometimes bought) as well as many I haven't but might be interested in. Behind the scenes, pixels are at work. Home Depot has more than a dozen tracking pixels on its web site. Those pixels pass my browsing and buying behavior to ad platforms. Those platforms then use that data in their ad products. This pixel-based approach to data sharing creates value for a number of parties:

- First, and most obviously, Home Depot wins because they measure the performance of their ads by understanding which ads led to purchases on their site. Home Depot can also improve the performance of its campaigns by running highly targeted ads.
- Ad platforms win because they earn more for ads that work better. They're also able to enrich their profile of me, which allows their machine learning algorithms to deliver more effective ads for not just Home Depot, but for all of their advertising customers.
- I'm arguably a winner too, because ad platforms show me ads that are more likely to be relevant to me. Thanks to the exchange of data about my interests, I will now see more home improvement ads instead of ads for products and services that either seem randomly selected,

or that may be cued by something less relevant, like the particular content of the page I happen to be visiting.

Of course it's not all upside. While most Americans quite reasonably haven't spent the time to understand the mechanics at play, they know full well that their data is being shared – and most people are uncomfortable with this fact. While it may be the case that no laws have been broken, it's fair to say that the data sharing underpinning this discomfort is a violation of people's reasonable expectation of privacy.

The scale of data collection and transfer using these mechanics is difficult to comprehend. Millions of web sites and apps have dozens of trackers installed. As a result, my behavioral data is collected by hundreds, perhaps thousands, of companies. Once data about my particular interests, activities and transactions is captured by entities that may or may not have a relationship with me, and have no particular loyalty to me, it's totally out of my control.

The unfortunate by-product of a system like this is at the heart of the central privacy problem plaguing digital advertising. We can call this "the profiling problem." In the model I've just described, ad platforms and advertisers have strong economic incentives to participate in this digital advertising system – and are disadvantaged compared to their competitors if they don't participate. As a result of this system, ad platforms are able to build tremendously rich profiles about their user base including most of your browsing and buying behavior.

To be clear, I'm not calling out the ad platforms categorically for having bad motives. I believe there are many good actors in the ad tech ecosystem that understand the potential harms caused by the development of these profiles. The challenge is this: without clear rules (e.g. laws and regulations) ad tech companies are highly incentivized to gather and use data as aggressively as possible. Proactively

eliminating the collection and use of third party data (e.g. pixel data) would put a platform at a massive disadvantage because ads that are data driven are just far more effective than those that are informed only by context or broad demographics. To address this incentive problem, we need to level the playing field by establishing clear criteria for what is and isn't acceptable.

Creating this level playing field requires a combination of efforts from legislators, regulators, advocates and technology companies. We believe there are three critical components that must come together to produce sustainable progress on digital privacy:

- 1) **Federal privacy legislation**, and supporting regulations, to provide baseline protections for all Americans and put an end to the race to the bottom in terms of data collection and use
- 2) **Strong enforcement authority** and action to make sure good actors aren't unduly disadvantaged when they take the initiative to improve their privacy practices
- 3) **Privacy enhancing technologies**, which, which will support massive advances in consumer privacy while ensuring advertising can continue to help businesses grow and keep content free

We've covered the importance of regulations and enforcement, given the incentives at play in the ad tech ecosystem, so now I'll focus on the technologies that can support a transition to a far more private approach to advertising.

How Privacy Enhancing Technologies Work

Privacy enhancing technologies (PETs) are a fairly broad class of technologies that enable confidential and private computing. PETs are used in many other industries and contexts. Financial services firms use them to collaboratively build fraud models without compromising individuals' data by sharing it directly with other companies. Pharmaceutical companies use PETs to bring together disparate data sets to conduct clinical trials while ensuring no party has access to sensitive healthcare information.

The Census Bureau uses PETs to support research on census data without compromising individuals' privacy. In the context of advertising, PETs can be employed to support three key use cases:

- Measurement: Understanding how ads lead to outcomes like purchases
- Targeting: Serving ads to individuals likely to have specific characteristics or interests, such as runners, mothers of young children or university students
- Optimization: Improving the relevance and effectiveness of advertising by using algorithms to make ad delivery decisions in an automated manner

To support these use cases, one must match two sets of data, one from the ad platform with information about who saw the ads and the other from an advertiser with information about actions on the advertiser's site or app.

Historically, the advertiser information has been sent directly to the ad platform, which is what creates "the profiling problem" I discussed earlier. With a PET-based approach, however, the profiling problem can be nipped in the bud – instead of one party directly sharing data with the other, the data is processed by an intermediary that itself has no access to unencrypted data. All computation happens in a fully safe and encrypted environment.

Inside this secure system the two data sets are joined and computations take place – including measurement and correlations that create aggregated data and statistics (in the example above, an advertiser like Home Depot might learn that 4% of men my age who saw the ad ended up buying the product).

Importantly, however, after completing the computation and generating trusted aggregated results, the individual-level data used to generate those results is deleted. The aggregated results of these computations are then further anonymized by using privacy mechanisms such as [Differential Privacy](#),

which adds noise (effectively random data) to limit the likelihood that individuals can be re-identified using the aggregated results.

The aggregated and anonymized results are then shared with the advertiser and the ad platform. The end result is that everyone gets what they need, but no party has learned anything new about any individual. This is the promise of privacy enhancing technologies, and this is the model we have been building at Anonym.

Summary

In summary, we believe the notion that you cannot have both privacy and an efficient digital advertising ecosystem that support businesses of all sizes is a false dichotomy. We believe in a win-win set of solutions that includes (but is not limited to) the following:

- Increased protections for children and older minors beyond COPPA, which was enacted in an earlier era when the internet and its content was frequently analogized to television – hence the focus on age 13.
- A single federal statutory scheme that provides a baseline for how data is treated and that strongly limits or prohibits sharing of individual consumer data directly between companies.
- Unified protections that operate the same way in all states to provide protections to all Americans. We support ADPPA because it provides these unified consistent protections.
- Strong and clear enforcement authority for privacy regulators.
- Technology that guarantees privacy while still empowering businesses to operate efficiently, find customers and grow.
- Importantly, to keep incentives clean and encourage competition, these technology solutions should be open and transparent and operated by companies that do not sell data or advertising.

Bringing these critical elements together will be a powerful demonstration of how government, citizens, businesses, and advocates can work together to establish a law-driven, technology-backed baseline for data privacy protection. We believe this will provide a global roadmap for how regulation and technology can work hand in hand to respect people's fundamental right to privacy while enabling quality consumer experiences and supporting economic growth.

Thank you again, Chairman Bilirakis, Ranking Member Schakowsky, and the other honorable members of this committee for your time and attention. I look forward to answering any questions you may have about my testimony or about these issues generally.

Mr. BILIRAKIS. Thank you. Thank you, Mr. Mudd. Appreciate it very much.

Ms. Givens, you are recognized for 5 minutes.

STATEMENT OF ALEXANDRA REEVE GIVENS

Ms. GIVENS. Thank you, Mr. Chair, and thank you, committee members, for the opportunity to testify on the importance of data privacy and the urgent need for Congress to pass a meaningful Federal privacy law to protect consumers, create certainty for businesses, and restore trust in the online ecosystem that is so essential to our economy and our society.

I am Alexandra Reeve Givens, and I have the privilege of leading the Center for Democracy and Technology, a nonprofit, nonpartisan organization that defends civil rights, civil liberties, and democratic values in the digital age.

For over two decades, CDT has advocated for Congress to adopt strong privacy protections, and we are grateful for the work of this committee and its jurisdictional counterparts in raising public understanding of privacy harms.

By our count, this is the 31st hearing in the U.S. Congress on consumer privacy in just the past 5 years, substantive hearings that have built a rigorous and detailed record about the overwhelming need for a comprehensive Federal privacy law. We commend the committee's focus on this issue early this session because it is long past time for Congress to act.

Looking for information on your device can feel very private, but with every click and scroll, companies collect information about your activities, typically using, sharing, or selling that information to make inferences about you or so you can be targeted with ads. A visit to a single web page can involve hundreds or even thousands of cookies or beacons tracking your activities on that site. Websites you have visited and search queries you have entered can be collected and shared.

In addition to your cell phone provider knowing your general whereabouts, apps on your phone can track and may share your location with anyone willing to pay a price, revealing where you live and work, where you socialize, what doctors you visit, and where you pray.

Consumers also share an incredible amount of personal and private information with different apps and online services, whether it be details about our physical health, our sleep cycles, our mental health, or social messages and family photographs.

In addition to direct collection by companies, all of that data can now be shared with third parties, such as data brokers, which are companies that aggregate information about users and market it, primarily for targeting ads. The huge variety and scale of data points gathered by data brokers allows precise inferences to be drawn about individual users.

A 2013 report by the Senate Commerce Committee details how data brokers assign profiles to people, including categories like "suffering seniors," "rural and barely making it," and "ethnic second-city strugglers." A report published by researchers at Duke University just last month revealed that data brokers were selling mental health information, including, for example, a list titled

“Consumers with Clinical Depression in the United States.” This committee published a report on privacy concerns raised by data brokers as early as 2006, but these practices haven’t been reined in.

When consumers learn about companies’ lax data practices, they are offended, but the issue is about more than just offensive stereotyping or privacy leakage. It can lead to social, psychological, and economic harm. It might not seem all that important if a person is targeted with particular clothing ads, but it matters when predatory lenders can hypertarget an audience that is vulnerable to payday loans and exploitative interest rates, as has happened with veterans and families navigating medical crises. It matters when scammers can target their ads to seniors who are more likely to fall for schemes hawking low-cost medical devices. It matters when inferences about people are used to unfairly target ads for jobs, housing, or credit, the gateways to economic and social opportunity.

My written testimony details how loose data practices can also raise national security harms.

The lack of a comprehensive Federal privacy law is leaving consumers open to exploitation and to abuse. Under current law, Americans’ main privacy protections rely on a theory of notice and consent under which companies can set their own privacy rules and collect whatever data they like, provided they disclose it to their customers in their lengthy terms of service.

Any modern user of technology knows why this notice and consent model is broken. Even if a consumer could feasibly read and understand these labyrinthine privacy policies, they often have no real choice but to consent. Many online services are such an important part of everyday life that quitting is effectively impossible. We have to move on from this broken regime of notice and consent to one that establishes baseline safeguards for consumers’ information, clear rules of the road for businesses, and meaningful enforcement of the law. This must include specific protections for sensitive information and protections for civil rights.

The bipartisan American Data Privacy and Protection Act is the place to start. Last year, this committee did admirable work forging a bipartisan compromise that offers strong protections for consumers while also accommodating business realities. To be clear, CDT and other consumer groups wished the bill offered stronger protections in places. This is not our perfect bill, but this committee put in the work to achieve meaningful compromise. Respectfully, we urge you to build on that momentum by taking up the bill without delay.

I thank the committee again for your leadership, and I look forward to answering your questions.

[The prepared statement of Ms. Givens follows:]

**Testimony of Alexandra Reeve Givens, Center for Democracy & Technology
One Page Summary**

1) *How Current Commercial Data Practices Harm Consumers*

- We share a vast amount of information with apps and online websites in the course of our daily lives. All of that data can be collected and stored indefinitely by companies, and sold to data brokers, which aggregate information and market it for ad targeting, among other uses.
- These practices can cause social, psychological, and economic harm. For example, predatory lenders can target an audience that is vulnerable to payday loans and exploitative interest rates. Ads for diets and dangerous weight loss medications persistently target people with histories of disordered eating, leading to depression and self-harm. Scammers can target ads to seniors. Inferences about people have been used to unfairly target ads for jobs, housing or credit. Other harms can also result, like when a fitness app revealed secret information about the location and layouts of U.S. military bases. There can also be national security concerns.

2) *The Need for Comprehensive Federal Privacy Legislation*

- While some companies have taken important steps to protect their users' privacy, the lack of a comprehensive federal privacy law is leaving consumers open to exploitation and abuse.
- Under current law, Americans' primary comprehensive privacy protections are based on the Federal Trade Commission's limited Section 5 authority, which typically turns on a "notice and consent" approach that allows businesses to do what they want provided they disclose it in their (lengthy) privacy policy. This solution simply is not workable in the modern age.

3) *Elements of a Comprehensive Federal Privacy Law*

- There are several elements essential to any meaningful federal privacy law:
 - Data minimization requirements that restrict companies to collecting and using only data that is necessary for the services they perform
 - Specific protections for sensitive data
 - Civil rights protections and algorithmic transparency and assessment provisions
 - Data security requirements
 - Rights for consumers to access, correct, delete, and port data pertaining to them
 - Meaningful, easy-to-use mechanisms for consumers to opt-out of data profiling for persistent targeted advertising
 - Children's protections that take into account the inability of children to protect themselves against exploitative data practices
 - Limits on sharing or selling data with third parties, including a national registry for data brokers and the right for consumers to delete data about them held by a data broker, and
 - Meaningful enforcement by the Federal Trade Commission, State Attorneys General, and a private right of action.
- The ADPPA reflects a well thought through and valuable bipartisan compromise, building on years of work by this Committee and its Senate counterpart. We encourage the Committee to take it up again without delay.

Testimony of Alexandra Reeve Givens
President & CEO, Center for Democracy & Technology

For the U.S. House of Representatives Energy & Commerce Committee,
Subcommittee on Innovation, Data, & Commerce
Hearing Entitled “Promoting U.S. Innovation and Individual
Liberty through a National Standard for Data Privacy”

March 1, 2023

Thank you Chair Bilirakis, Ranking Member Schakowsky, and Chair Rodgers and Ranking Member Pallone of the full committee for the opportunity to testify on the importance of data privacy, and the urgent need for Congress to pass a meaningful federal privacy law to protect consumers, create certainty for businesses, and restore trust in the online ecosystem that is so essential to our economy and our society.

I am Alexandra Reeve Givens, President and CEO of the Center for Democracy & Technology, a nonprofit, nonpartisan organization that defends civil rights, civil liberties and democratic values in the digital age. For over two decades, CDT has advocated for Congress to adopt strong privacy protections. We were one of the first organizations to propose a comprehensive privacy framework in the aftermath of the Cambridge Analytica scandal, when it was revealed that the data of almost 90 million Facebook users was collected without their consent by a political consulting firm to create profiles of people to more precisely target political advertising. Even in the short time since then, the public understanding of privacy harms has changed significantly, in part thanks to the work of this Committee and its Senate counterpart. By our count, this is the 31st hearing held in the U.S. Congress on consumer privacy in just the past five years: substantive hearings that have built a rigorous and detailed record about the overwhelming need for a comprehensive federal privacy law. We commend the Committee’s focus on this issue early in the new Congress, because it is long past time for Congress to act.

This morning, I plan to briefly describe how the current commercial data ecosystem is harming consumers, how the current legal regime governing online privacy has failed to keep up with innovation, and why the U.S. needs a significant shift in how we protect consumer privacy and the use of consumers' data through passage of a meaningful federal privacy law.

i. *How Current Commercial Data Practices Harm Consumers*

Looking for information on your device can feel very private, but with every click and scroll, companies collect information about your activities, typically using, sharing or selling that information to make inferences about you or so you can be targeted with ads. A visit to a single webpage can involve hundreds or even thousands of cookies or beacons tracking your activities on that site, both from the company you are visiting ("first party" tracking) and from mostly unknown third parties ("third party tracking").¹ Websites you have visited and search queries you have entered can be collected and shared. In addition to your cellphone provider knowing your general whereabouts, apps on your phone can track and may share your location with anyone willing to pay a price – revealing where you live and work, where you socialize, what doctors you visit, and where you pray to people and companies you have never heard of or interacted with.² Those apps may have no business collecting that information except to target advertising. Apps and websites are even fingerprinting your device and web browser to more precisely identify you and to circumvent both technical protections and consent requirements for cookies.³ Consumers also share an incredible amount of personal and private information

¹ Dan Rafter, *Tracking Cookies: What Are Tracking Cookies and How Do They Work?*, Norton (May 6, 2021), <https://us.norton.com/blog/privacy/what-are-tracking-cookies>.

² Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>.

³ Chiara Castro, *Web trackers: What they are and how to protect from them*, TechRadar (June 21, 2022), <https://www.techradar.com/features/web-trackers-what-they-are-how-to-protect-from-them> ("Browser fingerprint: With cookies getting more regulated - in some countries websites *must* allow users to choose to enable them or not - new tracking techniques are rising. Every browser connected to a certain device brings with it some unique data, including device model, screen resolution, operating system, language,

with different apps and online services, whether it be details about our physical health, our sleep cycles, our mental health, or social messages and family photographs.⁴

All of that data (and inferences companies make about consumers based on that data) can be collected and stored indefinitely by companies, and they can share it with third parties such as data brokers, which are companies that aggregate information about users and market it for, among many things, targeting ads.⁵ The huge variety and scale of data points gathered by data brokers allows precise inferences to be drawn about individual users. A 2014 report by the Federal Trade Commission described how data brokers assigned profiles to people based on the detailed information collected across the web, assigning users to categories like “Expectant Parent,” “Diabetes Interest” and “Smoker in Household.”⁶ A 2013 report by the Senate Commerce Committee detailed how dataset titles included categories like “Suffering Seniors,” “Rural and Barely Making It,” “Ethnic Second-City Strugglers” and “Rough Start: Young Single

browsing history, and so on. That defines its own browser fingerprint, which can then be used to track down your online activities every time you open the browser.”).

⁴ Mozilla, *Top Mental Health and Prayer Apps Fail Spectacularly at Privacy, Security* (May 2, 2022), <https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security> (detailing how apps that deal with private consumer information, such as health ailments, routinely have poor privacy practices).

⁵ Companies also use the data for fraud detection and credit check services, and sell data to law enforcement. See Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, *Legal Loopholes and Data for Dollars*, Center for Democracy & Technology (Dec. 2021), <https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf>.

⁶ Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014), at 42-43, <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

Parents.”⁷ This Committee explored these concerns in a report as early as 2006, and also held a hearing that addressed data broker practices in 2019.⁸

These data broker practices have not been reined in. A report published by researchers at Duke University just last month revealed that data brokers were selling mental health information, in some cases tied to consumer identities, including whether someone has depression, insomnia, or ADHD, among other medical conditions.⁹ Data brokers made available 28 types of medical data, and 42 types of non-medical data about consumers. These categories include data from wearable medical devices, specific medications, income, credit score, Social Security Numbers, and information about children.¹⁰ Data brokers are still grouping people and selling those lists, including specifically a list entitled “Consumers with Clinical Depression in the United States.”¹¹ The logic, said one data broker, is to exploit that data to specifically target people with medical ads based on their illnesses: “households with ailments are more likely to be interested in targeted offers about medical needs.”¹²

In addition, advertising trackers can detect specific and often personal information that users share with any given site. Last December, *The Markup* found that, out of the 50 telehealth

⁷ Staff Report, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, S. Committee on Commerce, Science & Transportation (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

⁸ See Internet Data Brokers: Who Has Access to Your Private Records?, Hearings Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 109th Cong. (2006); Protecting Consumer Privacy in the Era of Big Data, Hearing Before the Subcomm. on Consumer Prot. and Commerce of the H. Comm. on Energy and Commerce, 116th Cong. (2019). <https://www.congress.gov/event/116th-congress/house-event/108942>.

⁹ Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, Duke University Sanford Cyber Policy Program (Feb. 2023), at 9, <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf> (“some firms clearly advertised data already directly linked to individuals, as they offered individual names, addresses, and various forms of contact information (such as phone numbers and emails) in a dataset.”).

¹⁰ *Id.* at 20, app’x. B.

¹¹ *Id.* at 14.

¹² *Id.*

websites they analyzed, 13 of them contained at least one tracker that collected patients' answers to medical intake questions.¹³ Trackers on 25 sites told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan.¹⁴ Since then, the U.S. Department of Health and Human Services has clarified that use of tracking technologies like cookies by entities covered by the Health Information Portability and Accountability Act (HIPAA) are subject to the HIPAA privacy and HIPAA security rules.¹⁵

When consumers learn about these practices and how careless companies are with consumer data, they are often gravely offended. But the issue is about more than just offensive stereotyping or privacy leakage – it can lead to social, psychological, and economic harm. It might not seem that important if a person is targeted with particular clothing ads. But it does matter when predatory lenders, for example, can hyper-target an audience that is vulnerable to payday loans and exploitative interest rates, as has happened with veterans and families navigating medical crises.¹⁶ It matters when ads for diets and dangerous weight loss medications can persistently target people with histories of disordered eating, leading to depression and

¹³ Todd Feathers, Katie Palmer, & Simon Fondrie-Teitler, “*Out of Control*”: *Dozens on Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, The Markup (Dec. 13, 2022), <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>.

¹⁴ *Id.*

¹⁵ See Department of Health and Human Services, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (HHS/OCR December Bulletin highlighting the important privacy obligations health providers - such as doctor's offices and hospitals - are required to follow when using apps and websites, under the Health Information Portability and Accountability Act, which limits how your doctor or insurer can share patient health information).

¹⁶ Office of Representative Katie Porter, *AWOL: How Watchdogs are Failing to Protect Servicemembers from Financial Scams* (2021), https://porter.house.gov/uploadedfiles/va_home_loans_final.pdf; Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, Duke U. Sanford Cyber Policy Program (2021), <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf>. See also Coulter Jones, Jean Eaglesh, & AnnaMaria Andriotis, *How Payday Lenders Target Consumers Hurt by Coronavirus*, Wall Street Journal (June 3, 2020), <https://www.wsj.com/articles/how-payday-lenders-target-consumers-hurt-by-coronavirus-11591176601>.

self-harm.¹⁷ It matters when scammers can target their ads to seniors who are more likely to fall for schemes hawking low-cost medical devices.¹⁸ It matters when inferences about people are used to unfairly target ads for jobs, housing or credit, the gateways to economic and social opportunity.¹⁹

Even when online platforms prevent advertisers from targeting audiences on their platform using explicit protected categories such as race, gender or age, research has shown how easily “interest categories” and other means of audience targeting can serve as proxies for those characteristics.²⁰ We have long known that zip code can be a proxy for race,²¹ but so can a person’s identified interest pages, the websites they have visited, or their likes. To give just one example, it is easy to determine someone’s religion from the Facebook pages they have liked, which will often denote the church or faith community to which they belong.

Other harms can result from loose commercial data practices. In 2018, it was revealed that a fitness app was inadvertently revealing secret information about the location and layouts of U.S. military bases because personnel were recording their exercise regimes and sharing it with the application. Following a public outcry, the company made changes to its platform, and I am sure military personnel now receive stronger briefings on privacy protections. But the example

¹⁷ Liza Gak, Seyi Olojo, & Niloufar Salehi, *The Distressing Ads That Persist: Uncovering The Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating* (2022), <https://doi.org/10.48550/arXiv.2204.03200>.

¹⁸ AARP, *Medical Equipment Scams* (Mar. 2022), <https://www.aarp.org/money/scams-fraud/info-2019/medical-equipment.html>.

¹⁹ See Dept. of Justice, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising* (June 2022), <https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known>.

²⁰ Till Speicher *et al.*, *Potential for Discrimination in Online Targeted Advertising*, Proceedings of Machine Learning Research, Conference on Fairness, Accountability, and Transparency (2018), <http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf>.

²¹ Madeline St. Amour, *ZIP Codes and Equity Gaps*, Inside Higher Ed (July 2020), <https://www.insidehighered.com/news/2020/07/09/report-finds-racial-equity-gaps-college-attendance-debt-and-defaults-based-zip-codes>.

illustrates the revealing nature of location information, and the inadequacy of requiring users to be the sole guardians of their privacy, when it is often hard for users to know how an app will collect, use, or share their data with the world.

Security experts and members of this Committee have raised additional concerns over the national security effects of sharing data with other countries, including China. The permissive nature of the current U.S. privacy framework allows for data to be collected and shared by companies with impunity, which could be helped by imposing substantive guardrails on commercial data practices through federal privacy reform.

ii. *The Need for Comprehensive Federal Privacy Legislation*

While some companies have taken important steps to protect their users' privacy, the lack of a comprehensive federal privacy law is leaving consumers open to exploitation and abuse. Under current law, Americans' primary comprehensive privacy protections are based on the Federal Trade Commission's limited Section 5 authority over unfair and deceptive practices. Under Section 5, the primary mode of enforcement has relied on a theory of notice and consent, under which companies can set their own privacy rules and collect whatever data they like provided they disclose it to their customers.

Any modern user of technology can understand why this "notice and consent" approach is inadequate. Companies typically give notice to consumers through long privacy policies, often buried deep within the fine print of their terms of service. One academic study showed that a person would need to spend 244 hours to read all the privacy policies they encounter in a single year.²² Even if a consumer does read and understand the privacy policies, their choices are

²² Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 1/S: A Journal of Law and Policy for the Information Society (2008), https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf; Geoffrey A. Fowler, *I Tried to*

limited: either accept the service's terms, or do not use it. But many online services like internet service providers and social media companies are such an important part of everyday life that quitting is effectively impossible—and often there are few, if any, alternatives to use instead. If a social media service is the only way a consumer stays in touch with family and friends, asking them to quit is unreasonable.

Nor are countless pop-up windows asking a user to “accept or reject” a company’s privacy practices the answer, as Europeans have found after the European Union’s passage of the largely consent-based General Data Protection Regulation (GDPR). Users find these pop-up windows annoying and hard to navigate, and companies often establish default settings that funnel users into accepting less privacy-protecting options.²³ There is a rich academic literature about dark patterns, the ways in which privacy notices, consent boxes, and other design elements of a website or app can nudge consumers to accept certain policies through design choices intended to induce consent, even when the consumer would otherwise take the more privacy-protective action.²⁴ Dark patterns include misleadingly positive language, omitting details of how a person’s data will be used or shared, or adding friction to privacy interfaces that make it hard for users to find how to change their settings.²⁵

Read All My App Policies. It Was 1 Million Words, Wash. Post (May 31, 2022), <https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/>.

²³ Colin M. Gray *et al.*, *The Dark (Patterns) Side of UX Design*, Proceedings of the 2018 CHI Conf. on Human Factors in Computing Systems, Paper 534, at 5 (2018), <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108> (“Nagging behaviors may include pop-ups that obscure the interface, audio notices that distract the user, or other actions that obstruct or otherwise redirect the user’s focus.”).

²⁴ See, e.g., Jamie Luguiri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. Legal Analysis 43 (2021), <https://academic.oup.com/jla/article/13/1/43/6180579>; Lauren E. Willis, *Deception by Design*, 34 Harvard J. L. Tech 116 (2020), <https://jolt.law.harvard.edu/assets/articlePDFs/v34/3.-Willis-Images-In-Color.pdf>; Johanna Gunawan, Amogh Pradeep, David Choffness, Woodrow Hartzog, and Christo Wilson, *A Comparative Study of Dark Patterns Across Mobile and Web Modalities*, Proceeding of the ACM on Human-Computer Interaction, https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Gunawan-Pradeep-Choffness-Hartzog-Wilson-A-Comparative-Study-of-Dark-Patterns-Across-Mobile-and-Web-Modalities.pdf.

²⁵ Federal Trade Commission, *Bringing Dark Patterns to Light* (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

Against this backdrop, it is no surprise that consumers have lost trust in online companies.²⁶ Consumers are worried about their data and their privacy online, but are powerless to control that privacy.²⁷ They know they are being tracked by companies.²⁸ Consumers also have little confidence that companies will admit when they misuse data.²⁹

This lack of trust is bad for the economy, for businesses, and for consumers, as they feel powerless and like their only recourse is to simply stop using certain products and services—which many have.³⁰ But it doesn't have to be that way. Consumers have been asking for years for the government to protect their privacy.³¹ It is time to heed that call.

²⁶ See, e.g., Orson Lucas, *Corporate Data Responsibility: Bridging the Consumer Trust Gap*, KPMG (Aug. 2021), at 1, <https://advisory.kpmg.us/articles/2021/bridging-the-trust-chasm.html> (stating that 40% of consumers do not trust companies to use their data ethically).

²⁷ See e.g., Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> (81% of consumers say they lack control over what types of data companies collect; 81% say the risks of companies collecting data outweigh the benefits; 59% say they lack understanding of how companies use data); *Most Americans say it is increasingly difficult to control who can access their online data*, Ipsos (Jan. 2022), <https://www.ipsos.com/en-us/news-polls/data-privacy-2022> (“Seven in ten (70%) Americans agree that controlling who can access their online personal information has become more challenging”).

²⁸ Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans concerned, feel lack of control over personal data collected by both companies and the government*, Pew Research Center (Nov. 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/> (72% think all or mostly all of what they do online is tracked by companies).

²⁹ Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> (79%).

³⁰ *Most Americans Say it is Increasingly Difficult to Control Who Can Access Their Online Data*, Ipsos (Jan. 7, 2022), <https://www.ipsos.com/en-us/news-polls/data-privacy-2022> (36%).

³¹ Privacy for America, *New Data Reveals Americans' Overwhelming and Bipartisan Support for Federal Privacy Legislation* (Nov. 18, 2021), <https://www.privacyforamerica.com/new-data-reveals-americans-overwhelming-and-bipartisan-support-for-federal-privacy-legislation/> (stating 92% of voters want a privacy law).

iii. *Elements of a Comprehensive Federal Privacy Law*

Congress can make the U.S. a global leader by passing meaningful comprehensive privacy legislation, building on the foundational work of this Committee, its Senate counterpart, and Republican and Democratic administrations over more than a dozen years.³² The most important thing Congress can do is free consumers from a regime that primarily relies on notice-and-consent as a privacy protection. We need privacy laws that work in the 21st century digital economy, that give consumers the baseline protections they need and create clear rules of the road for businesses. As discussed below, we also need to ensure any privacy law can be effectively enforced.

There are several elements of a federal privacy law that would address the harms I have discussed today and significantly increase consumer trust:

- Data minimization requirements that restrict companies to collecting and using only data that is necessary for the services they perform,
- Specific protections for sensitive data such as biometric information, location information, health information, or information revealing someone's race, religion, sexual orientation, and similar factors,
- Civil rights protections and algorithmic transparency and assessment provisions to prevent companies from discriminating against people based on protected characteristics,
- Data security requirements ensuring that companies take steps to avoid data breaches and other unauthorized access to data,
- The rights for consumers to access, correct, delete, and port data pertaining to them that is held by a company,
- Effective, easy-to-use mechanisms for consumers to opt-out of targeted advertising,

³² Congressional Research Service, *Privacy Protections for Personal Information Online* (April 2011), https://www.everycrsreport.com/files/20110406_R41756_d4893c5a84e54603899b9471b9d853219c03424a.pdf. ("Beginning with the 109th Congress, every Congress has held numerous privacy-related hearings. The current Congressional privacy agenda is broad and includes items that Congress has worked on for several years, new issues posed by advances in technology, and items related to efforts to update the electronic surveillance laws for advances in technology.").

- Children’s protections that take into account the inability of children to protect themselves against exploitative data practices,
- Limits on sharing or selling data with third parties, including a national registry for data brokers and the right for consumers to delete data about them held by a data broker, and
- Meaningful enforcement by the Federal Trade Commission, state Attorneys General, and a private right of action.

Last year, this committee passed in an overwhelmingly bipartisan fashion the American Data Privacy and Protection Act (ADPPA), which includes all of these protections and more. CDT commends the Committee for its tireless work on that bill. To be clear, it is not a perfect bill. For instance, we would like to see narrower preemption of state laws and a broader private right of action, and higher penalties for data brokers failing to register. But we recognize that to ensure bipartisanship, compromise is necessary. ADPPA represents a reasonable middle ground for protecting privacy and civil rights online, and we encourage this Committee to take it up again without delay.

iv. Ensuring Meaningful Enforcement

It is essential that any privacy law passed by Congress can be meaningfully enforced and can keep up with rapidly changing innovations in commercial data practices. Given the complexity and scale of the modern digital ecosystem, this can be achieved only through a complementary approach that empowers the Federal Trade Commission, State Attorneys General, and a private right of action for consumers to enforce their rights.

The expert staff of the FTC is well positioned to bring cases involving data privacy harms. Congress should ensure, however, that the FTC is properly resourced to handle enforcement of a new privacy law. Investing in the FTC is good for consumers who receive more money in refunds

from FTC enforcement,³³ and good for the federal government because, according to an analysis from the Congressional Budget Office, every dollar invested in the FTC reduces the deficit by over three dollars.³⁴ Congress should also ensure the Commission provides resources to help businesses understand their obligations and pursue responsible data practices, for example by staffing a resource center.

Even with greater resources, federal enforcers cannot possibly keep up with the entire ecosystem of commercial data practices. State Attorneys General can and should play an essential role in protecting consumers' privacy, building on the existing expertise many have demonstrated in fraud, privacy, data security, and digital civil rights. In addition to bringing enforcement actions, Attorneys General frequently work with business leaders and advocacy organizations to identify concerns about products and services and to develop best practices, playing a vital role in protecting consumers' interests.³⁵ Finally, a private right of action is essential. Even with multiple levels of government enforcers, resource constraints will limit effective application of the law. Consumers should have the ability to be made whole through the court system if their issues are not taken up by government enforcers. A private right of action would help ensure that people's wrongs can be made right.

³³ Since 2018, for every dollar invested in the FTC, consumers have been refunded \$2.44. See Federal Trade Commission, FTC Appropriation and Full-Time Equivalent (FTE) History, <https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation> (showing FTC funding between 2018 and 2022 at \$1.675 billion); Federal Trade Commission, *Data on Refunds to Consumers*, https://public.tableau.com/app/profile/federal.trade.commission/viz/Refunds_15797958402020/RefundsbyDate (showing total refunds between 2018 and 2022 at \$4.1 billion).

³⁴ Congressional Budget Office, *Estimated Budgetary Effects of Title III, Committee on Energy and Commerce, H.R. 5376, the Build Back Better Act* (Nov. 18, 2021), <https://www.cbo.gov/publication/57623> (showing that a \$1 billion investment in the FTC over the course of ten years equates to a reduction in the deficit by \$3.1 billion).

³⁵ Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 759 (2016). See also Senate Commerce Committee, Testimony of Laura Moy (Oct. 10, 2018), at 12-13, <https://www.commerce.senate.gov/services/files/baf68751-c9bc-4b15-abof-d4a5f719027c>.

v. Why Congress Must Also Address AI and Automated Decision-Making

A final issue I would like to highlight is the need to address artificial intelligence and automated decision-making. Increasingly, AI systems that leverage large amounts of data are being used in decisions about employment, lending, tenant screening and other settings that can dramatically impact people's lives.³⁶ These tools raise significant risks of bias, lack of transparency, and unfair decision-making. In particular, these issues come up when tools evaluate people based on factors that do not actually relate to the decision in question (causing hidden errors and unfair outcomes), or when they make inferences about people that approximate protected characteristics such as race, gender, religion, or disability status (perpetuating bias and discrimination).

The ADPPA takes a meaningful step in the right direction. It increases transparency into algorithmic systems, used by large data holders, to help people, regulators, legislators, and others to understand what the purpose of the AI system is, how it was designed, and the steps the company has taken to mitigate various foreseeable harms. More public and detailed information will better inform policymaking going forward.

Thank you very much for your time and I look forward to your questions.

³⁶ See, e.g., Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021), <https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms>; Pranshu Verma, *AI is Starting to Pick Who Gets Laid Off*, Wash. Post (Feb. 20, 2023), <https://www.washingtonpost.com/technology/2023/02/20/layoff-algorithms/>.

Mr. BILIRAKIS. Thank you so very much. Appreciate it.
 Ms. Rich, you are recognized for 5 minutes.

STATEMENT OF JESSICA RICH

Ms. RICH. Thank you, Chairman Bilirakis and Ranking Member Schakowsky, and the rest of the members of the committee. I am Jessica Rich, of counsel and senior policy advisor for consumer protection at Kelley Drye & Warren. I am pleased to be here today testifying on the need for Federal privacy legislation.

I really want to thank this committee for its bipartisan leadership on this important issue over the course of years. I also want to make clear that my remarks today are my own, based largely on my years of government service.

As background, I worked for over 26 years at the Federal Trade Commission, the last 4 as Director of the Bureau of Consumer Protection. Much of my FTC career was devoted to data privacy and security. I was the first manager of the FTC's privacy program and continued to lead its expansion as I rose through the ranks at the agency.

In my various roles, I developed or oversaw enforcement against hundreds of companies that failed to protect consumers' personal information, rulemakings to implement privacy laws, such as the Children's Online Privacy Protection Act, and dozens of FTC workshops and reports on emerging issues.

During my time there, I also wrote or oversaw multiple recommendations to Congress, seeking stronger legal authority and remedies for privacy and security. The years have come and gone with multiple hearings and privacy bills. And as we all know, there is still no Federal privacy law over two decades later.

Today, the need for a Federal privacy standard has never been greater, and there is no substitute for congressional action here. Federal privacy legislation is simply the best way to create a consistent set of rules for consumers and businesses, fill in the many gaps in our privacy patchwork, enlist multiple enforcement in policing the marketplace, and provide much-needed credibility abroad. Although I could expand on every single one of those points, I am going to focus today on a related issue, which is why the FTC needs a Federal privacy law.

As much as the FTC has been able to do with the tools it has, it needs more authority from Congress to be a truly effective privacy enforcer. In fact, under current law, the FTC's legal authority is limited, whether it is pursuing case-by-case enforcement under the FTC Act or attempting to develop a privacy regulation. I will explain why briefly here, but I refer you to my written remarks for more details.

First, because there is no comprehensive Federal privacy law, the FTC has had to bring most of its privacy enforcement under section 5 of the FTC Act, a general-purpose consumer protection law enacted long before the internet existed or was even thought about. Section 5 prohibits unfair or deceptive practices, and each of these standards has a three-part legal test.

Sometimes the legal tests simply don't work for privacy because they weren't written with privacy in mind. For example, to prove unfairness, the FTC must show that a practice causes or is likely

to cause substantial consumer injury, which can be very difficult in privacy where injury can be very subjective and there is a range of different types of harms.

In addition, section 5 doesn't establish clear standards for companies to follow before a problem occurs. It is mostly reactive, allowing the FTC to challenge data practices afterwards.

Finally, the FTC Act doesn't authorize civil penalties for first-time violations, and it doesn't even cover nonprofit entities or companies engaged in common carrier activities. Now, the FTC is attempting to plug at least some of these holes by developing a privacy regulation, and in theory an FTC privacy regulation could set forth practices that companies must follow—do this, don't do that—and also pave the way for civil penalties.

But this approach faces even more obstacles in case-by-case enforcement, and it will use up the FTC's limited resources too. That is because, without specific direction from Congress to develop a privacy rule, the FTC must rely on its rulemaking authority under the FTC Act, which is also called Magnuson-Moss rulemaking.

The Mag-Moss process—we all have a nickname for it—is extremely cumbersome and time consuming as compared with the usual rulemaking process under the Administrative Procedures Act. For example, Mag-Moss requires the FTC to prove that each practice it seeks to regulate is not only unfair or deceptive but prevalent. Mag-Moss also includes an extra round of public comments, public hearings, and a more rigorous standard for judicial review. Rules developed under this process have typically taken years to complete, and with all the controversy surrounding privacy, we can also expect legal challenges here. There is simply no substitute for Federal privacy legislation.

Congress can write a law that says “do this, don't do that.” It can plug the holes in the FTC Act, as well as in the U.S. privacy patchwork that we all know overall, and only Congress can resolve the thorniest issues here and put them to rest: preemption and the private right of action.

Thank you very much. I look forward to your questions.
[The prepared statement of Ms. Rich follows:]

STATEMENT OF JESSICA RICH

**Of Counsel and Senior Policy Advisor for Consumer Protection
Kelley Drye & Warren LLP**

Before the

**Subcommittee on Innovation, Data, and Commerce
Committee on Energy and Commerce
United State House of Representatives**

On

**“PROMOTING U.S. INNOVATION AND INDIVIDUAL LIBERTY THROUGH A
NATIONAL STANDARD FOR DATA PRIVACY”**

March 1, 2023

I. INTRODUCTION AND BACKGROUND

Chair McMorris Rodgers, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky, and members of this Subcommittee, I am Jessica Rich, Of Counsel and Senior Policy Advisor for Consumer Protection at Kelley Drye & Warren, and a Distinguished Fellow at Georgetown University. I am pleased to be here today, testifying before this Subcommittee on setting a national standard for data privacy. I want to thank this Committee for its leadership and ongoing efforts on data privacy issues. I also want to make clear that my remarks today are my own, based largely on my years of experience in government service.

My background is as a lawyer and law enforcement official. I worked for over 26 years at the Federal Trade Commission (FTC), the last four as Director of the Bureau of Consumer Protection, overseeing the agency's efforts to protect consumers from harmful marketing, advertising, and data privacy and security practices. Much of my FTC career was devoted to data privacy and security. I was the first manager of the FTC's privacy program, starting in the late 1990s, and led its expansion as a division manager, and later as Deputy Director and then Director of the Bureau of Consumer Protection. In my various roles, I developed or oversaw enforcement against hundreds of companies that failed to protect consumers' personal information; rulemakings to implement privacy laws such as the Gramm-Leach-Bliley Act (GLBA),¹ the Children's Online Privacy Protection Act (COPPA),² and the Fair and Accurate Credit Transactions Act (FACTA);³ and educational and policy initiatives to highlight emerging issues and promote best practices.

I also wrote or oversaw multiple recommendations to Congress seeking stronger legal authority and remedies for privacy, starting in 2000⁴ and then echoed and refined in subsequent years.⁵ I left the agency in 2017, but I have continued to press for a federal privacy law in Congressional

¹ 15 U.S.C. § 6801 et seq.

² 15 U.S.C. § 6501 et seq.

³ 15 U.S.C. § 1681 et seq.

⁴ *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000) ("2000 Report"), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

⁵ See, e.g., *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policy-makers>.

testimony, op-eds, and speeches because of its importance to consumers, businesses, the FTC, and my longtime commitment to the issue.⁶

II. THE NEED FOR A COMPREHENSIVE FEDERAL PRIVACY LAW

I am here today to plead the same case yet again. The need for a federal privacy law has never been greater, and there is no substitute for Congressional action here. For over two decades, Congress has debated the issue. While Congress did pass some sector-specific legislation like COPPA and GLBA, it has repeatedly failed to act on comprehensive legislation. Meanwhile, Europe and countries all over the world moved ahead with detailed data protection laws, as have five U.S. states, with more in the pipeline.⁷ All states now have data breach notification laws;⁸ about half have data security laws;⁹ and many also have sector-specific laws, like Illinois' Biometric Information Privacy Act.¹⁰

This “patchwork” (as it is so often called) is confusing and costly for consumers and businesses alike, and getting more so. Consumers need a strong and consistent law to protect them across jurisdictions and market sectors, and to clarify what privacy rights they should expect and demand as they navigate the marketplace. Businesses – especially small and medium sized ones – need to know what the rules are without having to spend millions of dollars on attorneys and overly complex compliance schemes. We have just the opposite now – a rolling wave of new and disparate privacy laws that confuse everyone and require an armada of experts to interpret.

Federal privacy legislation is the best way – and indeed the only way – to create a consistent set of rules that protect consumers nationwide. It will bring clarity for consumers and businesses; level the playing field between large and small companies; cast a wide net of protection that can

⁶ See, e.g., *Give the FTC Some Teeth to Guard our Privacy*, New York Times Op-Ed (August 2019), <https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html>.

⁷ See IAPP State Privacy Legislation Tracker, <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.

⁸ See *Security Breach Notification Laws* (National Conference of State Legislatures or “NCSL”), <https://www.ncsl.org/technology-and-communication/security-breach-notification-laws>.

⁹ See *Data Security Laws – Private Sector* (NCSL), <https://www.ncsl.org/technology-and-communication/data-security-laws-private-sector>.

¹⁰ 740 ILCS 14.

address issues like discrimination and the misuse of kids' and teens' data; significantly boost enforcement and remedies for violations; and provide much-needed credibility abroad.

Although I could expand on each of the above points, my testimony today will focus on a related issue that is just as important – which is why *the FTC* needs a federal privacy law. As much as the FTC has been able to do with the tools that it has, it needs more authority from Congress to be a truly effective privacy enforcer. That's why the FTC has asked Congress so many times to pass federal privacy legislation. That's also likely why all three of the FTC's Democratic Commissioners, even as they launched their Section 18 (a/k/a "Mag-Moss") rulemaking on Commercial Surveillance and Data Security¹¹ (hereinafter "Privacy Rulemaking"), stated or implied that they would back away from the rulemaking if Congress were to pass a comprehensive privacy law.¹²

Indeed, under current law, the FTC's authority is limited, whether pursuing case-by-case enforcement or attempting a Mag-Moss rulemaking. Only Congress can establish the kind of broad-based protections contained in recent privacy bills such as the ADPPA. And only Congress can put to rest the issues that have been debated for years – notably whether to preempt state privacy laws and/or grant a private right of action, and how much discretion the FTC should have to shape the requirements (i.e., through rulemaking). Below, I provide more details about some of the strengths and limits of the FTC's privacy authority.

III. THE FTC'S PRIVACY AUTHORITY

1. Background on the FTC's privacy program

The FTC built its privacy program almost entirely around Section 5 of the FTC Act, a law that was written long before the arrival of the Internet.¹³ That's because, in the mid-1990s, when the Internet

¹¹ See *Commercial Surveillance and Data Security Rulemaking*, <https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking>.

¹² Despite her support for stronger federal privacy mandates, Republican Commissioner Wilson dissented from the rulemaking, stating that Congressional action is the best course. All of the Commissioners' statements can be found at <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices>.

¹³ 15 U.S.C. Sec. 45.

did arrive, there were very few U.S. laws (federal or state) that specifically addressed privacy. After holding hearings on what the Internet would mean for consumers and competition, the FTC quickly recognized that privacy would be a serious concern. It therefore sought to use Section 5, its general law prohibiting “unfair or deceptive” practices, to address this issue.¹⁴

Since then, the FTC has used Section 5 to challenge the data practices of a wide range of companies, including retailers, data brokers, mortgage companies, pharmacies, software companies, mobile apps, and most of the major tech companies.¹⁵ The cases have spanned a wide range of fact patterns, too – false or misleading data privacy and security statements or settings,¹⁶ including about children’s data,¹⁷ breaches of financial¹⁸ and health information,¹⁹ and even personal data about extramarital affairs;²⁰ spyware in people’s homes;²¹ and a wide range of other alleged violations.

The FTC has bolstered this enforcement, and increased its influence and visibility, with frequent use of the “bully pulpit” – including workshops and reports highlighting emerging issues and recommending best practices; consumer and business guidance; and testimony and

¹⁴ See *2000 Report*, supra at n. 4, for discussion of the FTC’s early privacy efforts.

¹⁵ See *Privacy and Security Enforcement*, <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement>. There is a misperception that the FTC shied away from using unfairness until recently. In fact, many of the FTC’s data privacy and security cases have been based on unfairness.

¹⁶ See, e.g., *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (“Facebook Settlement”), <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>.

¹⁷ See, e.g., *FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors*, <https://www.ftc.gov/news-events/news/press-releases/2000/07/ftc-sues-failed-website-toysmartcom-deceptively-offering-sale-personal-information-website-visitors>.

¹⁸ See, e.g., *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers Data*, <https://www.ftc.gov/news-events/news/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx-data-brokers-reed-elsevier-seisint>.

¹⁹ See, e.g., *Electronic Health Records Company Settles FTC Charges It Deceived Consumers About Privacy of Doctor Reviews*, <https://www.ftc.gov/news-events/news/press-releases/2016/06/electronic-health-records-company-settles-ftc-charges-it-deceived-consumers-about-privacy-doctor>.

²⁰ See, e.g., *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users’ Profile Information*, <https://www.ftc.gov/news-events/news/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting-2015-data-breach-exposed-36-million>.

²¹ See, e.g., *FTC Halts Computer Spying*, <https://www.ftc.gov/news-events/news/press-releases/2012/09/ftc-halts-computer-spying>.

recommendations to Congress.²² Often, the FTC faced strong headwinds from industry and members of Congress, who opposed, not only the FTC's efforts, but any attempts to strengthen federal privacy laws.

Although Congress passed some sectoral privacy laws in the late 1990s and early 2000s (including COPPA, GLBA, and FACTA), the FTC Act continues to serve as the agency's core legal authority in privacy, given its broad scope relative to the sectoral laws. Most of the cases brought against the large tech companies, for example, were based on Section 5.²³

Significantly, though, virtually all of the FTC's privacy and data security cases are settlements. That means that many of the legal theories advanced, as well as the remedies obtained, have never been tested in court.²⁴

2. Limits of Section 5

The FTC's success in building a substantial and influential data privacy and security program can sometimes mask the limits of its legal authority in this area. In fact, Section 5 was not designed for privacy and is ill-suited for it in various ways. On the one hand, it has provided the FTC with substantial flexibility to tackle a wide array of practices. But on the other, the concepts of "deception" and "unfairness" contain many gaps and shortcomings when it comes to privacy. These shortcomings have become increasingly problematic as data use has proliferated and become more complex.

As a reminder, to prove deception, the FTC must show that there is a material representation, omission, or practice that is likely to mislead a reasonable consumer.²⁵ To prove unfairness, the FTC must show that a practice causes or is likely to cause substantial injury to consumers that

²² See *FTC Policy Work on Privacy and Data Security*, <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/ftc-policy-work>.

²³ See, e.g., *Facebook Settlement*, *supra* at n. 16; *Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, <https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples>.

²⁴ One notable exception is the *Wyndham* case, in which the 3rd Circuit upheld the FTC's authority to challenge lax data security practices as unfair. *FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 240 (2015).

²⁵ *Policy Statement on Deception*, <https://www.ftc.gov/legal-library/browse/ftc-policy-statement-deception>.

cannot reasonably be avoided by consumers, and is not outweighed by countervailing benefits to consumers or competition.²⁶

One challenge is that Section 5 (and associated case law) was developed with traditional commercial transactions in mind – such as when a company sells, and a consumer purchases, a product or service (such as a sweater, tractor part, or investment) for a particular purpose and the consumer does not receive the goods or services intended or expected. In such situations, privacy may not be top-of-mind for consumers as they consider the transaction, even if they care about it in a general sense. In the case of the sweater, consumers may be thinking about its appearance, fit, or fabric, not whether the company stores credit card numbers securely, or sells consumer data to third parties. This can make it difficult to show that privacy was *material* to a consumer’s decision to purchase the product or service.

Another challenge is that proving a practice “causes or is likely to cause” substantial injury for purposes of unfairness has always been a conundrum in privacy, especially since the concept of privacy injury can be so subjective. Is emotional or reputational injury sufficient? Is the mere release of data (even sensitive data) enough? How sensitive must data be to have its sale or compromise rise to the level of “likely” substantial injury? The FTC’s Unfairness Statement (which courts still cite in their opinions) says that “emotional impact” and other “subjective” types of harm will not ordinarily make a practice unfair, but might do so in “extreme cases” when “tangible injury” can be shown.²⁷ Similarly, the Supreme Court has held that “concrete harm,” and not the “mere risk of future harm,” is necessary to confer standing to plaintiffs in privacy class actions.²⁸ The FTC must continuously navigate the issue of harm when it comes to privacy.

Yet another problem is that Section 5 does not establish clear standards for companies to follow before problems occur – it is almost wholly reactive. It does not tell businesses, for example, what privacy disclosures and choices they need to provide to consumers, or what data uses are so

²⁶ 15 U.S.C. § 45(n). The statutory test, enacted by Congress in 1994, superseded the FTC’s Policy Statement on Unfairness (“Unfairness Statement”), <https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness>. However, the FTC and the courts still refer to portions of the Policy Statement, especially its discussion of consumer harm, and many of its principles are baked into FTC case law.

²⁷ See *Unfairness Statement*, *supra* at n. 26.

²⁸ *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

inherently risky or harmful that they should be avoided or modified. Instead, it allows the FTC to evaluate a company's practices after the fact, to determine whether they meet the unfairness and/or deception tests. (The FTC is trying to fix this problem by promulgating its Privacy Rule, but that faces obstacles of its own, as discussed below.)

In addition, certain requirements that appear in existing privacy laws and bills are an especially poor fit for Section 5. Is the failure to provide access or deletion rights to consumers, without more, deceptive or unfair? What about a company's failure, without more, to audit its practices using certain criteria, or to have its executives attest to the audit? Certainly, companies have agreed to these types of requirements in settlements (as so-called "fencing-in" to prevent the companies from committing additional violations in the future) but that doesn't mean that failure to take these steps meets the deception and/or unfairness tests, or that a court would make that determination.

Finally, the FTC Act does not cover non-profits or companies engaged in common carrier activities – limitations that have long created an obstacle to even-handed FTC enforcement. Nor does it authorize civil penalties for first time violations or, since *AMG*, allow the FTC to seek consumer redress in federal court under Section 13(b).²⁹ (A rulemaking would lay the groundwork for monetary relief, but cannot alter the FTC's jurisdictional limits.)

3. Magnuson-Moss rulemaking

The FTC is well aware of the limits discussed above. That's why it has repeatedly, on a bipartisan basis, asked Congress to pass a federal privacy law that includes specific privacy mandates; authority to obtain civil penalties; and jurisdiction over nonprofits and common carriers.³⁰

Congress has not acted, which is frustrating for many. So after two decades of asking, the FTC has moved ahead on its own, by launching its Privacy Rulemaking under Mag-Moss.

²⁹ Given the difficulty of quantifying many types of privacy injuries, penalties are often the better remedy.

³⁰ See, e.g., *FTC Report to Congress on Privacy and Security* (September 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf; Prepared Remarks of Chairman Joseph J. Simons on "Oversight of the Federal Trade Commission: Strengthening Protections for American's Privacy and Data Security," <https://www.ftc.gov/legal-library/browse/prepared-remarks-chairman-joseph-j-simons-oversight-federal-trade-commission-strengthening>.

The Mag-Moss process is more cumbersome than “normal” rulemaking under the Administrative Procedures Act (APA). That’s because Congress deliberately added provisions to make it so, due to perceived overreach by the FTC in the 1970s (especially its proposal to ban TV food advertising to kids – known as “kid vid”).³¹ Of particular note, Mag-Moss requires the FTC to prove that each practice it seeks to regulate is unfair or deceptive, as well as prevalent. In other words, the FTC is confined to the very same legal standards that, as discussed above, create obstacles for privacy – and must prove prevalence, too.

Mag-Moss also includes an extra round of public comments, public hearings as requested by stakeholders, and a more rigorous standard for judicial review.³² According to a professor who analyzed FTC rules developed under Mag-Moss, the average time it took to complete them was almost six years, versus less than a year for APA rules.³³

In addition, a sometimes-forgotten Mag-Moss provision limits the FTC’s authority to develop rules regarding kids’ advertising. This provision, now found in Section 18(h) of the FTC Act, prohibits the FTC from promulgating “any rule in the children’s advertising proceeding pending on May 28, 1980” (i.e., ‘kid vid’) or in any “substantially similar proceeding” based on unfairness.³⁴

In July 2021, an FTC majority voted to simplify the Mag-Moss rulemaking procedures, to the extent that it could, by stripping away some steps that the FTC had previously added to the process through its own internal rules.³⁵ However, most of the cumbersome requirements appear in the law, which the FTC cannot change. In addition, the Commission appears to be charting an ambitious path forward in the Privacy Rulemaking, one that portends a very long process. In its first request for comment (the Advance Notice of Proposed Rulemaking, or ANPRM), the FTC

³¹ See, e.g., *The FTC as National Nanny* (Washington Post Editorial, March 1, 1978, at A22).

³² 15 U.S.C. § 57a.

³³ Jeffrey Lubbers, *It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking* (G.W. Law Review, February 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2560557.

³⁴ 15 U.S.C. § 57a(h).

³⁵ *FTC Votes to Update Rulemaking Procedures, Sets Stage for Stronger Deterrence of Corporate Misconduct*, <https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-votes-update-rulemaking-procedures-sets-stage-stronger-deterrence-corporate-misconduct>. Among other things, the changes eliminated the need for a staff report analyzing the rulemaking record, and gave the Chair more authority to control the public hearings process.

discussed dozens of privacy topics, posed 95 questions, and touched on many controversial issues. Not surprisingly, the agency received over 11,000 comments from the public.

The obstacles here are enormous. To develop a rule of the breadth that Congress considered in the bipartisan ADPPA, the FTC would need to prove that many dozens of practices are both prevalent and unfair or deceptive, with all of the associated challenges discussed above. It must review and analyze thousands of comments (twice) and hold public hearings with numerous stakeholders clamoring to be heard. Even if the FTC is able to complete the rulemaking, litigation seems likely, whether based on the particular issues regulated or bigger picture questions about the FTC's legal authority here.³⁶

Additionally, the FTC cannot resolve (or should not be the one to resolve) the most controversial issues in the privacy debate – whether to preempt state laws,³⁷ grant a private right of action, and/or impose limits on its own rulemaking discretion. Nor can it address the data practices of common carriers and non-profits – those entities would not be covered by an FTC rule.

IV. CONCLUSION

There is simply no substitute for federal privacy legislation. No other U.S. privacy regime or proposal can create the broad protections and consistent standards that the U.S. sorely needs. Congress must finally pass a federal privacy law to protect and reassure the American public.

³⁶ Multiple comments on the FTC's ANPRM argue that the FTC's proposal raise concerns under the "Major Questions" doctrine recently discussed by the Supreme Court in *West Virginia v. EPA*, 142 S. Ct. 2587 (2022).

³⁷ In theory, the FTC could try to preempt state privacy laws, or set its Privacy Rule as floor that the state laws could exceed (as it has proposed to do in its rulemaking to ban non-compete clauses). See e.g., *Fidelity Savings & Loan Assn. v. De La Questa*, 458 U.S. 141 (1982). However, any such proposal would likely draw legal challenge.

Mr. BILIRAKIS. Thank you very much. I appreciate it.

I thank all of the witnesses for their testimony today. Excellent testimony, by the way.

We will now move into the question-and-answer portion of the hearing. I will begin the questioning and recognize myself for 5 minutes.

Thank you again to the panel. We have made clear the American people deserve to have more control over their data, and we are hard at work to pass comprehensive privacy and data security legislation to do just that. But we are also committed to this effort because businesses, especially small and medium-sized businesses, need certainty. They should not live in fear of spending their time and resources to legal compliance to survive in the digital economy.

Unfortunately, the opposite is occurring, and the growing State patchwork is unsustainable for the American economy. And California is still adding more layers to the regulation.

Ms. Rich, you referenced the FTC's current privacy rulemaking in your testimony. I want to highlight that their rulemaking would not preempt State laws, meaning more regulatory uncertainty. How will adding another layer to the current patchwork lead to negative economic impact and a disruption for small and medium-sized businesses to operate?

Ms. RICH. I agree that that would be problematic, especially since the FTC can't work through the difficult issues related to preemption that this committee and Congress can.

Mr. BILIRAKIS. Thank you very much.

Mr. Mudd, would you like to comment on this, please?

Mr. MUDD. Sure. You know, I think it is absolutely the case, Congressman, that a patchwork of State legislation really does hurt smaller businesses and particularly smaller publishers more than it does larger ones. Larger tech companies have armies of engineers that can adjust their technologies State by State, jurisdiction by jurisdiction. That is just not possible for smaller publishers and companies.

Mr. BILIRAKIS. Thank you.

Ms. Rich, protecting all Americans from unfair and deceptive acts is no small undertaking. As you may know, the ADPPA included a section for FTC-approved compliance mechanisms for small businesses who may have difficulty complying with a law. I know safe harbors have also helped the FTC in their ability to enforce laws.

Can you speak more on that and explain why safe harbors would be helpful to the FTC and legislation such as the ADPPA?

Ms. RICH. Thank you. If done right, safe harbors or compliance programs can increase compliance overall while also providing the certainty and the flexibility that certain—that businesses, especially small and medium-sized businesses, need. The idea is that an independent organization can create a compliance program that meets or exceeds the standards in the law. And then the FTC approves them using a rigorous process, and then companies that need this kind of structure and guidance and help can join the program and be evaluated and certified for compliance, and thus comply with the law. If the requirements are rigorous, which they are

in the ADPPA, it expands both compliance while also providing certainties for the companies that joined these programs.

Mr. BILIRAKIS. Very good. Thank you very much. I will yield back.

And now we will ask the ranking member of the subcommittee, I give her 5 minutes for her questions. Thank you.

Ms. SCHAKOWSKY. First of all, let me just say how cheered I am by the consensus that we have. You know, we have got a practitioner, we have got a not-for-profit, we have got government. We have got, it seems, Republicans and Democrats, so let's move forward.

So the question—let me start with Ms. Givens. So it seems to me that the current notice and consent privacy regime really doesn't work very well for consumers. So is there a better approach, and how would you describe that?

Ms. GIVENS. Thank you for the question. And you are absolutely right that the current model of notice and consent is broken. And I think any person that uses the internet or a device today knows that, right? We are forced to click through long terms of service that many people do not stop and take the time to read. And even if we could take the time to read them, consumers don't feel like they have a choice. Often we need to be able to access a service to communicate with friends or family, for example.

So instead, what we need is the model pursued in the ADPPA, which is strong baseline protections for consumers' data that don't rely on somebody clicking through on whatever a company has chosen to disclose in its terms of service, but instead provide baseline protections and rules of the road. These include things like protections for data minimization. So the assumption that companies can only collect, process, and share data in the course of delivering the service that the user expects, as well as heightened protections for sensitive areas of data which can include anything from precise location information to health data, for example, to other biometric information.

Those are the types of rules that we need to give customers confidence again in the online ecosystem and also help businesses know how to govern their practices.

Ms. SCHAKOWSKY. Thank you.

So, Mr. Mudd, I also want to talk to you about the burden that I think is really right now on the consumers themselves, the notice and consent regime, but how does this play in the ad tech world? I mean, do you know anybody who reads all of the—I mean, I once brought in the pages and pages of the terms of service and all of that. So I just wondered how you would comment on what we need to do better. And I don't want to see more burdens then saying the consumer has to do more to protect themselves.

Mr. MUDD. I couldn't agree more. I do believe that the current approach is wholly insufficient in protecting consumers. And I think your assumption that the vast majority of people do not read privacy policies or terms of service is, of course, correct and, therefore, that consumers do not understand how data that they admit is being used, transferred, collected, et cetera.

Ms. SCHAKOWSKY. So what do you do to help the consumers? How is your business different?

Mr. MUDD. As Ms. Givens pointed out, I think the whole point of the technologies that we and others are developing is to just raise the baseline, to not allow the kinds of data sharing that have taken place in the past, as opposed to asking consumers, putting the work on them to make decisions that they are not well informed to make and they certainly don't have the time or inclination to focus on. And so it is all about privacy by default, data minimization, moving the bar up, instead of putting the work on the consumer.

Ms. SCHAKOWSKY. Yes. And let me ask you, Ms. Rich. So what you are talking about is that we have the tools or we can have the tools through the Federal Trade Commission. And how important, then, do you think is the role of the FTC as our regulator?

Ms. RICH. Oh, the FTC as the regulator here is critical. They have been doing this work for 25 years. They have enormous sophistication about the issues. They have the will to protect consumers, and they just need better tools, stronger legal tools to protect consumers across the marketplace.

Ms. SCHAKOWSKY. You know, I do have time, but I want to say that the witnesses that we have today I think can really be helpful to us as we move forward to make sure that the law that we did pass can be improved, can be made better, so that we can, during this Congress, get across the line that I think we have really come close to right now. And, you know, the United States of America really owes it, I think, to our consumers. We are just too far behind. We owe it to our children. We owe it to our families. We owe it to legitimate businesses to make sure that we—that we move forward.

So let me just say thank you very much. And I yield back.

Mr. BILIRAKIS. The gentlelady yields back. And I would like to say to the ranking member, you are right, we are too far behind, too far behind. That is the bottom line.

OK. Now I will recognize the vice chairman of the subcommittee, Mr. Walberg, for his 5 minutes of testimony.

Mr. WALBERG. Thank you, Mr. Chair. And I would certainly concur that we are far behind, but we take an early start here, and that is a good thing, as we have already talked about the patchwork of competing laws that are out there in the State level. And now we are working on something I think we can come together. We have shown that.

One area I think we can all agree is the need to address children's privacy. Republicans in the House are committed to putting parents back in the driver's seat, and even grandparents back in the driver's seat. Being a little personal there. It includes providing more tools to protect them online.

Kids' privacy has long been a priority for me. In past Congresses, I introduced bipartisan legislation that would update COPPA for our increasingly digital world, and the ADPPA included additional protections for those under the age of 17.

Ms. Givens, how should children's privacy protections be addressed differently than those for adults in the comprehensive privacy law?

Ms. GIVENS. Thank you for the question, and thank you for your leadership on this issue to protect children across the country.

The ADPPA includes some important protections for children, and it is specific in calling them out. One is the additional division created at the FTC to focus on this issue. But additionally there are protections, for example, prohibiting the targeting of ads to children and teenagers under the age of 17, and also express limits on the sharing of their information without expressed opt-in consent.

This matters because our children are being targeted online, and unfortunately COPPA right now is not up to the job in addressing abusive data practices. But what is critically important is that we can't just focus on the privacy needs of kids. We need to do this in a comprehensive way that protects all consumers. And the reason we need to do that is, when you only focus on protecting the interests of children, you actually create new obligations, for example, to test for people's ages, that can sometimes undermine people's privacy.

So what we need to do is the approach that is followed in ADPPA today, which is to lift up privacy protections for all consumers, and then charge those additional resources to protecting kids in additional ways, to make sure that we really are living up to what our children need online.

Mr. WALBERG. OK. What is good for one can be good for all in a great way as we do it comprehensively.

COPPA currently includes an actual knowledge standard for information, Ms. Rich, collected on those under age of 13. The law was passed in 2000, and the FTC last made rule changes in 2013.

How has the landscape changed since then, and is an actual knowledge standard still appropriate?

Ms. RICH. You went right to the heart of the issues, didn't you?

Mr. WALBERG. Sometimes I do it right.

Ms. RICH. Yes, yes. The FTC has not updated COPPA, and a lot of people wonder why. In remarks, public remarks, there was some suggestion that they are waiting to see if Congress updates the law so that, you know, they don't have to do it twice, but I can't fully understand why they are not using the tools that they have.

COPPA is very outdated. Information collection has just exploded even since 2013, and it was pretty considerable then, and all sorts of new practices in the marketplace. And we really do need special protections for kids and teens as is included in the ADPPA.

Mr. WALBERG. OK. Ms. Givens, in your testimony, you referenced a report by Duke University which was interesting, which revealed that data brokers were selling mental health information to advertisers. This included whether someone has depression, insomnia, Alzheimer's disease, other medical conditions. I read the same report or read the same report and am extremely concerned.

HIPAA was created to protect our medical information, but with the explosion of health apps, that data is no longer just held by your doctor's office. What gaps are there in protecting medical privacy, and how do we fill them?

Ms. GIVENS. Thank you for the question because this is an urgent problem. You are right that HIPAA does protect data, but it is only when it is held by a covered entity, which doesn't include any of the commercial apps or services that users interact with every day. Sometimes sharing really important mental health in-

sights, if you are using an app to kind of do, you know, journaling. And in addition, inferences that companies can make about you based on your behavior, from which they might be inferring some of the medical conditions that we just described, which is why we have to have——

Mr. WALBERG. True or untrue, yes.

Ms. GIVENS. Yes. So which is why we have to have a comprehensive privacy law to fill those gaps for all of the non-HIPAA-covered entities that are still making inferences and deductions about people's mental health status, as well as other medical conditions as well.

Mr. WALBERG. Thank you. My time has expired.

Mr. Mudd, I have another question, the best question you could ever have had, but I will submit it for the record.

Mr. MUDD. Sounds good.

Mr. BILIRAKIS. Thank you very much. I appreciate that.

And now we will recognize the gentleman from Florida, Mr. Soto, for his 5 minutes. Florida is very well represented on both sides of the aisle in this committee. It is just a coincidence, right?

Thank you. You are recognized. Go ahead.

Mr. SOTO. Thank you, Chairman. You are making Florida proud.

You know, it is nothing short of a mild miracle last term when we saw both parties come together to pass out of the committee the American Data Privacy and Protection Act. When you look at some of these key sections, like the sensitive covered data section, it reads really like an internet privacy bill of rights. Information that everyday Americans would think would already be protected is still subject to risk of being distributed and used for—in commerce, like people's Social Security numbers and health information, financial account information, debit card information, biometric information, genetic information, your precise geolocation at this very moment, your private communications like voice mails, emails, text messages and mail, account logins and passwords, identifying people's different behaviors socially, as well as calendar information, address book information, so many of the things that we would all shudder to know that could be sold and used for profit to help target people in a really intimate way that violates our notions of privacy in the Nation.

You know, Florida does not have internet privacy laws, even though we have a privacy amendment in our constitution. It has failed a couple times over enforcement disputes. So our State and 22 million Floridians are left vulnerable by not having rights, which is why it is time for us to step up to create a national standard. Not to mention that I can't think of anything more related to interstate commerce than the internet. So it is a really important time for us.

Ms. Givens, it would be great to get your opinion on this list of basic data covered, on these basic rights that we have, and do you think there should be any others added?

Ms. GIVENS. In my opinion, the ADPPA did an excellent job capturing many of the major categories of sensitive data. You listed many of them. And to the point that you made, these are things Americans already expect to be protected. They are horrified when they find out that it is not protected, and they want baseline safe-

guards in place to make sure that they can trust the services they consult online.

While the list is strong and good now, there needs to be ongoing flexibility to add to it in the future, because we know that the marketplace will continue to innovate. We cannot foresee what data uses may arise in the next 5, 10, 15, 20 years, which is how long, of course, this law would likely be in place in governing user behavior.

And so one of the important innovations in the bill is to leave some room for the FTC to fill in the gaps where needed and be responsive to emerging cases, which the FTC can do based on rule-making procedures, stakeholder consultation as new norms evolve. And that, I think, is the right approach that the bill takes today.

Mr. SOTO. So do you believe that already is included, that kind of flexibility is already enough in the ADPPA already for the FTC to recognize these new types of information?

Ms. GIVENS. I do think so. I think the covered list that we have now, the fact that it includes both the data itself and inferences that may reveal that information, coupled with the ability to fill in gaps in the future, is a really important combination.

Mr. SOTO. Thank you.

And, Ms. Rich, we know how important enforcement is. We saw in Florida that was the key sticking point that kept our State from actually having a new law. And I am very concerned that we don't end up having a toothless tiger here. The bill we already passed out of the committee last year had both a role for the FTC, a private right of action, and rules for State attorney generals.

How critical is it to have all three of these mechanisms in place, and can you give us any guidance on that?

Ms. RICH. Well, having been part of this debate for over 20 years, I would say whatever it takes for you guys to agree on a law is what I support. But I do think that some level of consistency is important and—which is why I do support some level of preemption and some limits on private litigation, especially since private litigation sometimes benefits attorneys more than consumers.

But I actually think the model in the ADPPA is very good because it empowers the FTC, it empowers not just all the State attorney generals but other officers in the State that might have a role in privacy. And so given that the State attorneys general have been very active in privacy, I think this new tool would empower them even more, and we have a lot of cops on the beat.

Mr. SOTO. Well, thanks for that opinion. You know, many tech companies are running circles around government enforcement right now. And so very important to have a balance, in my opinion, between FTC or State attorney generals and having some private right of action. Thank you for your opinions.

And I yield back.

Mr. BILIRAKIS. Thank you, sir. Appreciate it very much.

Now I will recognize the gentleman from South Carolina. Mr. Duncan, for his 5 minutes.

Mr. DUNCAN. Thank you, Mr. Chairman. And this has been an informative hearing. I am an energy guy, so this isn't in my wheelhouse, but it is educating me on the issue.

So just one real quick question, because, Ms. Rich, we have heard a lot from downtown over the preemption clause in the ADPPA, namely that it doesn't go far enough, especially with respect to overly restrictive provisions coming out of California. While the previous Speaker of the House disagreed with that sentiment, I understand there are concerns over certain carve-outs that are not otherwise addressed in the bill.

Could you speak to that?

Ms. RICH. Well, as I said, I do think that there is some level of preemption that should be in the bill so we get as much consistency as possible. I would also note that, by the measure of many consumer advocacy groups who are reading all of these bills and laws very carefully, the ADPPA is stronger than existing State laws, for the most part. It may be one provision here and there and stronger. But, you know, in an effort to compromise, this committee carved out certain things, including the California private right of action.

So as I said, whatever it takes, but I do believe the ADPPA is the strongest law we have seen—the strongest bill we have seen anywhere on privacy.

Mr. DUNCAN. Thank you for that.

I think some sort of uniformity where States know how to comply with a lot of different things, the ADPPA being an example of that.

Mr. Chairman, legislative hearings and hearings like this are very informative. I appreciate you doing that.

I don't have another question. I yield back.

Mr. BILIRAKIS. I appreciate that very much. Thank you.

And now I will recognize the ranking member of the full committee, Mr. Pallone, for his 5 minutes.

Mr. PALLONE. Thank you, Mr. Chairman.

I am concerned about data brokers collecting and selling massive and detailed amounts of information about consumers who have never interacted with these data brokers.

So let me start with Mr. Mudd. In your written testimony, you point out that the scale of data collection and transfer using online mechanics is difficult to comprehend. Based on your experience working in advertising technology, could you tell us what types of information data brokers have about consumers, how they collect that information, and what they do with it in about a minute or so?

Mr. MUDD. I will do my best.

So, in terms of the types of data that are collected by data brokers, it is, again, difficult to be comprehensive here. Certainly basic demographics: your age, your gender, your household composition and so forth. But certainly also well beyond that: your profession, the makeup of your household, the age of your children, the location, of course, of your household, oftentimes also your workplace, oftentimes even your real-time location, your income, and other financial statistics about you.

And then, of course, your behaviors. Your behaviors on the web through, you know, pixels, cookies, and so forth, as well as off the web in the real world. Retailers oftentimes will sell data about your shopping behavior to data brokers, who will then resell that data onward to others.

And then, as others have pointed out, health conditions are oftentimes also gathered and inferred as well.

Now, where do they get this information? Well, as of right now, there is very little constraint on how they can go about gathering it, and so they, of course, gather it from everywhere they possibly can. That means public databases. That means the websites that we interact with and so forth. It means, as I mentioned, real world, you know, retailers.

And then there are even, you know, specialty location companies that try to understand where you are in the physical world and share that data with brokers.

Mr. PALLONE. Thank you.

Well, let me have some followup on that with Ms. Givens.

Ms. Givens, are consumers aware of these data brokers? And do consumers have any practical options to tell data brokers to stop collecting or to delete their information? And does the American Data Protection and Privacy Act that we, you know, passed out of committee last Congress, does that take the right approach on data brokers?

Ms. GIVENS. So consumers are largely unaware of data broker practices and I think would be extremely hard pressed to name any. Part of the problem is that they operate in an opaque layer of the digital ecosystem and don't have to interact directly with consumers, which means they don't need to earn consumer trust.

Some data brokers allow users to opt out, and some States are beginning to require that they make this option available, but it is incredibly hard to exercise. First of all, you need to know who the data brokers are, and there are thousands of them. So even knowing where to go to opt out is a challenge.

Second, even if one is able to go through that interface, and often it involves many steps, you have to keep going back to do it again and again because the settings might change. They might collect new data over time.

So the ADPPA has some really important provisions on this. One is the data brokers need to disclose who they are, and they need to register with the FTC. So there is a one-stop shop for users to go and see who data brokers are.

Data brokers also need to comply if you opt out of sharing your information with them, and they need to have a centralized mechanism that allows opting out across the entire data broker ecosystem. That is hugely important for consumers to actually be able to influence and operate their rights.

Mr. PALLONE. All right. Thank you so much.

I have got a little over a minute left.

Let me ask Ms. Rich. Can you tell me about some of the most egregious practices you saw by data brokers in your time at the FTC?

Ms. RICH. Well, this is going to seem kind of old fashioned since companies can do so much more with data even than when I left the FTC in 2017. But selling data to con artists with reason to know it could be used for fraud. We had a bunch of cases like that.

Failing to secure sensitive data, leading to massive breaches. Many of the breach cases, especially in the early days, involved

data brokers who would amass all of this sensitive information, leading to identity theft when the data was breached.

Failing to vet buyers, leading to significant access to sensitive information by, you know, anyone that could pay. And, again, identity theft.

So these are—this is what we saw all the time, and, again, the marketplace is so much more sophisticated that, you know, I am sure there are all sorts of—a litany of other things that we could list that are even worse.

Mr. PALLONE. Thank you very much.

Thank you, Mr. Chairman.

Mr. BILIRAKIS. Thank you very much. I appreciate it.

I next will recognize the ranking member—excuse me—the chairman of the committee. She is wearing her E&C colors today.

Mrs. RODGERS. That is right.

Mr. BILIRAKIS. Well, we appreciate all of your great work.

And I recognize you for 5 minutes. Thank you.

Mrs. RODGERS. Thank you. Thank you very much, Mr. Chairman.

And, again, thank you to the panel for being here.

I wanted to start with an issue that we have been focusing on, debating over the last few years around targeted advertising.

Mr. Mudd, there is a particular line in your testimony which I think really hit the mark. And you said, “over the years, a tension began to emerge: the development of the rich consumer profiles that were so powerful in improving products of all kinds came at the cost of individuals’ privacy. This tradeoff is why we are here today.”

And I believe that you are right on that assessment, even if the online advertising industry doesn’t want to admit its reliance on personal information and freely flowing—following Americans as they browse the internet.

So the question is, do they really need personally identifiable information in order to facilitate the e-commerce? And you are suggesting that there is a middle ground here. So I just wanted to ask, would your privacy-enhancing technologies, also called PETs, permit innovation in the digital advertising ecosystem to continue? And how can PETs be used to help small businesses advertise to their customers without customers feeling that the businesses know too much about them?

Mr. MUDD. Thank you, Chair Rodgers.

Yes, we do believe that this is a reasonable middle ground and that it would protect from the flow and sharing of personally identifiable information from one company directly to another, which leads, as I mentioned, to the development of these very rich profiles, which we have talked a lot about today.

And the way that that happens is, you know, reasonably straightforward. What we need to do is ensure that only the aggregated anonymized insights that are required to understand how ads work and to improve their relevance are shared, not the individual-level data. That is not required.

To give an example in another industry, pharmaceutical trials. They need to bring data together from, you know, the drug companies, as well as the practicing physicians, but they don’t want to share individual-level data. They can use these exact same privacy-

enhancing technologies to understand whether the drug worked or didn't work, but they don't need the user-level data to do that. That is not important for the case.

Mrs. RODGERS. Thank you. Thank you.

Ms. Rich, you mentioned in your statement the importance of creating a regulatory climate that is conducive for businesses to be able to comply, and, you know, there is a lot that has been said about the negotiation that took place on ADPPA.

We included a right to cure in the private right of action to ensure businesses are able to comply with the law, and this is important so businesses are not buried underneath piles of demand letters seeking payments without the opportunity to cure an alleged violation, because I don't think any of us want to be there.

So would you speak to the benefits of a right to cure for businesses who face an alleged allegation?

Ms. RICH. Well, when I was at the FTC, I wouldn't have supported a right to cure because it does give people a second bite of the apple to, you know, violate the law, but when it comes to a private right of action and their concerns about the effect on, you know, companies that aren't the largest companies and can't afford all of this litigation, I think the right to cure is a very reasonable response to make sure that, instead of a private right of action leading to a lot of litigation, companies have a chance to get it right—one chance—and then comply and have the protections in place for consumers.

And I would note that other privacy regimes include rights to cure both for private right of actions and for government enforcement.

Mrs. RODGERS. Thank you.

Ms. Givens, I know that we may not see eye to eye on every aspect of ADPPA, but I do want to thank you for your support of our work.

A private right of action is a tough nut to crack in the scope of a bill like ADPPA. You highlight some of the boundaries of where FTC can enforce harms. In your testimony, you state the FTC's unfairness statement, which courts still cite in their opinion, says that emotional impact and other subjective types of harm will not ordinarily make a practice unfair but might do so in extreme cases when tangible injury can be shown.

So I am sympathetic for why there's strong desires to include a private right of action in such an instance when Big Tech may harm someone, especially a child. However, I also want to make sure that it is not abused by the plaintiffs' attorneys who would rather laws be so stringent so businesses are more likely to be out of compliance in order to sue.

Would you be willing to work with us to ensure that there are parameters for how the private right of action operates for businesses, especially businesses of different sizes?

Ms. GIVENS. Yes, Madam Chair. Of course, we are always happy to work with this committee.

A private right of action really is essential because the FTC and State AGs alone won't be able to keep up with the pace of commercial activity, and consumers deserve the right to be able to vindicate their rights when State enforcement aren't stepping in.

But, respectfully, the ADPPA already puts in a lot of protections to help small businesses and others from this risk of litigation, sometimes over the objection of consumer advocates in the negotiations. But the committee did an awful lot of work to get there.

Just to give a couple of examples, the private right of action only applies to some portions of the law and cannot be used against small businesses. In addition to that, there are limits on the damages that can be pursued. So right now the private right of action can only be used for compensatory damages and injunctive relief, not for statutory damages, which might remove a lot of the incentives for more speculative litigation.

In addition, you already mentioned the right to cure. There is also an obligation for any plaintiffs before they file suit or even send a demand letter to give notice to the FTC and to State Attorneys General in case either the FTC or State AGs want to bring the enforcement action instead. And there is a 60-day waiting period for that to happen as well.

When you couple that with restrictions the courts have already brought on standing, making it hard for consumer groups and class actions to be filed, there are a lot of protections that I think address the concerns that you have raised, coupled, finally, with the reporting obligation in the bill for the FTC to assess the impact on small businesses.

So, again, what we see here is the hard-fought compromise, but it is one that helps make sure consumers can vindicate their rights in some circumstances while mitigating the risks of abuse against small businesses or extraneous litigation.

Mrs. RODGERS. Thank you.

And, just to clarify, that was a quote. I was asking—I said—it was from Ms. Rich, but I appreciate you addressing and answering my question. Thank you.

Ms. GIVENS. I will take credit for her testimony any time.

Mrs. RODGERS. Thank you, Mr. Chairman. I yield back.

Mr. BILIRAKIS. I thank the chair. I appreciate it very much.

Next we have Mrs. Trahan. I recognize you for your 5 minutes of questioning.

Mrs. TRAHAN. Great.

Thank you, Mr. Chairman, Ranking Member Schakowsky, for organizing today's important hearing.

You know, like many of my colleagues on the dais, I am disappointed that we failed to pass the American Data Privacy and Protection Act in the full House last Congress, and I urge my colleagues, particularly those who are new to the committee, to continue working in a bipartisan way to pass a comprehensive privacy law that meets the needs of the families we represent.

Mr. Chairman, the Federal laws that govern our privacy today, in March of 2023, are the same ones that were in place when we had a hearing on holding Big Tech accountable a year ago in March 2022. They are the same laws that were on the books when the CEOs of Google, Meta, and Twitter testified before this same committee a year prior to that in March 2021.

In fact, they are the same laws that for decades have permitted companies to harvest our sensitive data. Things like medical symptoms that we look up on a search engine or our location that paints

a picture of where we work, where we send our kids to school, and where we pray, and sell that data to third parties or use it in ways that are contrary to what any of us would reasonably expect.

Many of us have been sounding the alarm about this for a while. In the past 2 years, I have sent inquiries to phone and messaging apps asking about the misuse and sale of messaging metadata to data brokers, about the sale of geolocation data, and to online gaming companies about their treatment of data collected on our teens. These companies can and should be doing better, but without comprehensive privacy legislation like ADPPA, they won't act.

And it doesn't stop there. One type of product I want to highlight the desperate need for an update is education technology. According to a 2021 study from Center for Democracy and Technology, 85 percent of teachers and 74 percent of parents believe EdTech is very important to students' education, and more teachers are becoming aware of the need to thoughtfully consider students' privacy.

However, a majority of parents still have concerns about student privacy, and a significant number of teachers still have not had training on privacy policies and procedures.

So, Ms. Givens, with the Family Educational Rights and Privacy Act, or FERPA, having passed nearly a half century ago, back in 1974, and still being the law of the land when it comes to student data, can you describe to what extent companies that offer EdTech software are or are not covered by FERPA?

Ms. GIVENS. Thank you for the question and for citing our report.

We spend a lot of time with educators, teachers in the classroom, as well as students and their families, and so we see firsthand the level of concern about how kids' data is being used in this environment.

To answer your question, FERPA applies to personal information from education records that are maintained by covered entities. That basically means public K through 12 schools, colleges, and universities that accept Federal student aid. When EdTech software vendors work with those covered entities, they have to comply with FERPA.

But, really importantly, FERPA falls short in all of the other ways in which EdTech vendors might be engaging and receiving information about students. So, first, it doesn't contemplate harms that might result from other types of information, like when the vendor interacts directly with the student and gathers that type of record.

Second, FERPA doesn't address any of the civil rights issues that can stem from algorithmic harms, as we are seeing increasing use of AI systems deployed in education settings.

And, third, FERPA's enforcement mechanisms fall directly on schools and not on the vendors, and the punishments are draconian. You lose your Federal funding.

We need the burden for privacy compliance to sit not just with the schools, which are so overwhelmed, but with vendors in this space as well. And so complementing FERPA with strong comprehensive privacy protections for those commercial uses of this technology is really important as well.

Mrs. TRAHAN. Thank you.

You know, in some cases, EdTech software is, as you mentioned, not offered through business-to-school contracts. Instead, they may be a free online game or an educational app, and the data collected while on these sites or apps can later be used to target ads or sold to third parties, particularly on our students who are 13 and older.

So the idea of consent gets murky, as you mentioned, when we are talking about a student or their parents deciding between participating in class while being tracked versus not participating at all. Can you speak to how the duty of loyalty and data minimization and ADPPA would be applied to these types of sites and apps?

Ms. GIVENS. You are exactly right. So FERPA only applies to vendors when they are processing education records, which doesn't include many of the many other ways that students are interacting with technology today.

I think about the experience with my own children, and they download apps, not going through those official channels. They are sharing a lot of information, and they are doing it to be able to have an educational experience. Again, this shows why notice and consent is broken as a model, because there isn't a question of consent. You want to be able to access these platforms.

And, sadly, COPPA is falling short here too, although, of course, it does offer some protection to services targeting children under the age of 13. That, too, essentially, rests on the notice and consent regime that is really hard to operationalize in practice.

So that is why we need the broader comprehensive privacy protection, is to regulate those additional uses and create baseline protections for students.

Mrs. TRAHAN. Thank you. Thank you so much for your testimony.

I yield back.

Mr. BILIRAKIS. Thank you. Thank you very much.

Next we will recognize Dr. Dunn from the great State of Florida.

Mr. DUNN. Thank you very much, Mr. Chairman.

I appreciate the opportunity to discuss the importance of advancing a bipartisan national privacy and data security bill. For years the FTC and the industry has been calling on Congress to enact a uniformed data privacy bill, and it is high time we did that. A national standard will provide all Americans certainty that their data is protected while providing clear rules for the road for businesses to follow.

But I know that this topic is incredibly complex, and it has to be carefully crafted to make sure that we protect Americans without stifling our innovation and our industry. Fortunately, the chairman and the ranking member have assembled a stellar panel of witnesses with outstanding qualifications in just exactly this very difficult area. So we are counting on the three of you to make this happen. No pressure.

During my time on the China Task Force last year, it became clear that the Chinese Communist Party poses a huge threat to the free world. All these digital areas, they cheerfully sabotage freedom and democracy everywhere they go, and this mentality permeates all of their corporations, including those that operate in America.

Ms. Givens, the Center for Democracy and Technology promotes civil liberties and democratic values in the digital age. To help pro-

vide context and clarity for our committee, can you briefly summarize the difference in the civil liberties and the fundamental values in the digital area, you know, between the CCP authoritarian system and our own system?

Ms. GIVENS. So I will admit that I am not a China expert, and I know that this committee had an important hearing last month that dove even deeper into these issues.

But I will tell you why we fight for privacy legislation as a question of American democracy, and the reason is, when consumers are trying to access information, when they are trying to communicate with their loved ones, when they are trying to find and share information and express themselves, they deserve a right to not be tracked and surveilled with every step, click, and scroll that they take.

People often talk about the right to privacy being the gating item that protects all of our other fundamental rights, our rights to expression, our right to access information, our right to associate with other people, and I deeply believe in that. We need those baseline protections for people to be able to exercise their democratic rights, and that is what makes this bill an important aspect for American values.

Mr. DUNN. I thank you for that.

In your testimony, you highlight the ways that data brokers assign profiles to people based on information they compile from multiple sources. I am concerned, by the way, that CCP could take advantage of this system to build highly individualized profiles on our Americans in general.

What would you say that current threat assessment is of the CCP accessing American citizens' data?

Ms. GIVENS. Well, the problem with the current digital ecosystem today is that consumers have no idea where that data is going, and it could be accessed by anybody: third parties, foreign intermediaries, foreign entities.

Mr. DUNN. So this is Threat Level Orange or higher?

Ms. GIVENS. And we need controls on that, and the way to do it is by minimizing the amount of data that companies have and putting restrictions on what data can be shared so that people actually can have confidence that, when they share something, it is not being accessed by those unknown third parties.

Mr. DUNN. Let me ask you another. So the ADPPA would require companies to notify individuals whether or not their data is collected by—and that is whether it is processed and transferred to, stored in any way accessible to China, in addition to a few other concerning countries.

Is this an adequate protection? Or should we be fencing this data just into America alone? I mean, how would we control data once it is outside our borders, whether it is in China or in a great ally like Canada? I mean, how does that happen?

Ms. GIVENS. Right. So I think the idea of fencing data is incredibly problematic. It is hard to operationalize. It raises much bigger questions.

Here the regime that you talked about in ADPPA provides notice about when data is being transferred to some particular named countries, but more important than that in my opinion are the data

minimization provisions in the bill, which say that, for everyone, let's be careful about how much data is collected in the first place and then let's impose restrictions on how that data is shared.

And that is the way to help rein in this unfettered sharing and access to information to any type of unknown party, including foreign entities.

Mr. DUNN. Excellent. Excellent.

Mr. Mudd, would you like to comment on the potential benefits of greater transparency by data collection for individuals? And does that represent challenges to the businesses in terms of complying with more transparency requirements?

Mr. MUDD. I think transparency is an important element of the solution, but by no means is it sufficient. I think it is important for consumers to certainly understand and have the access to the data that is collected about them, to control it and so forth, but as we have talked about at length here, it is really important to raise the baseline instead of just putting the work and the burden on consumers to understand the data collected and how they might use it.

Mr. DUNN. Thank you very much for your answers.

Mr. Chairman, thank you very much, and, Ranking Member, thank you very much for this meeting.

I yield.

Mr. BILIRAKIS. My pleasure. Thank you very much. Great questions.

We will recognize now Ms. Kelly from the State of Illinois. You are recognized, ma'am, for 5 minutes.

Ms. KELLY. Thank you, Mr. Chair, and Ranking Member Schakowsky for holding this hearing this morning.

I am encouraged that my colleagues on both sides of the aisle who agree that we must continue working on a national standard for data privacy for American consumers. Although I had hoped to get something in this space done last Congress, as we know, it is never too late to discuss such an important topic impacting all of our constituents' lives.

As we all know, almost everyone uses a smartphone, tablet, or laptop to complete mundane daily tasks, to order food, shop online, or simply search the web for entertainment. So I am especially interested in how data practices, which include companies sharing or selling consumer information, can be used to harm Americans.

Ms. Givens, you address this very concern at the top of your witness testimony. Can you explain some of the specific harms resulting from companies and data brokers using, sharing, or selling consumer information?

Ms. GIVENS. Absolutely. And thank you for the question.

As I outlined in my testimony, there are examples of how data brokers gather all of these different pieces of information across the web to create very detailed profiles on people and to lump them into categories, which is used for targeting of ads and other types of inference-based behavior. When we look at what some of those categories are, you can instantly see what the nefarious harm might be.

"Ethnic second-city dwellers," you know, "struggling seniors," this is offensive, but it also is showing why those ads might be tar-

geted to particular vulnerable populations, and that is the type of consumer harm that we need to be careful about, and we really need to try to rein in.

The other part is when ads are being targeted to people based on protected characteristics. That can be race, gender, religious, you know, religious identity, and many other factors or approximations of those factors. And that is another instance where we are seeing live instances of economic and social harm.

Ms. KELLY. Also, I am the founder of the Tech Accountability Caucus, and I want to dig into this issue around data purpose and use limitation. So I am interested in making it easy for consumers to understand when their personal information is being collected, how it is used and when and for what purpose it shared.

So, Ms. Givens, toward that end, in addition to requiring data minimization, do you think it would be beneficial to consumers for a Federal privacy framework to include a provision directing the creation of a list of standardized privacy categories and symbols aimed at providing simple, clear indications to consumers about how their data is being treated?

Ms. GIVENS. So we need baseline rules about how data can be used, but there also, of course, need to be elements about clarifying notices to consumers. We don't want to rely on notice alone because consumers can't keep up, but we do want consumers to better understand what practices are. And when there are moments to exercise their rights, to agree to a particular instance of data sharing, to be able to do that in an educated way and in an efficient way.

There is language in ADPPA now that talks about what their short-form notices are called. That is the term of art in the bill. But I do think that real guidance there about what that looks like, some standardized way of talking about this, perhaps the use of symbols to help people understand particular practices could go a long way in boosting consumer education and, therefore, having consumers feel more empowered.

Ms. KELLY. Thank you.

Lastly, as a Black woman and member of the Congressional Black Caucus, I am deeply concerned with the prevalence of discriminatory digital marketing and advertising. We know companies use different data points to discriminate against consumers and cause real harm.

Ms. Givens, I am going to give you a break.

Mr. Mudd and Ms. Rich, if you could answer this question: Are there certain use limitations, for example, that can curb discrimination and help protect civil rights, especially as it relates to protecting communities of color?

Ms. RICH. Absolutely. And the ADPPA, as you well know, includes antidiscrimination provisions that are remarkably powerful given where we have been in this debate, as well as assessment and auditing provisions to create greater transparency and accountability.

And I would note that many of those provisions—I mean, the FTC has stated that it can reach discrimination, but many of the provisions like accountability, assessment, executive accountability, the restrictions on targeted advertising, the data broker registry,

all these things we have been talking about would be very hard for the FTC to reach. Congress needs to do it.

Ms. KELLY. Thank you.

Mr. MUDD. I would agree wholeheartedly. I would say that it is absolutely reasonable and critical for sensitive data, race, gender, sexual orientation and so forth, to be treated very differently from, you know, other types of behavioral data, not just in its use but also its collection and sharing.

Ms. KELLY. Anything you want to quickly throw in? I am running out of time.

Ms. GIVENS. No. I will let my colleagues do the talking. Thank you.

Ms. KELLY. Thank you so much.

And I yield back my time.

Mr. BILIRAKIS. Thank you very much.

Next we will recognize the gentlelady from Arizona, my good friend Mrs. Lesko.

Mrs. LESKO. Thank you, Mr. Chairman.

And thank you to all the witnesses for being here today.

In-home connectivity has become a major selling point for homeowners, and voice-controlled personal assistance, such as Apple's Siri, Amazon's Alexa, and Google's Google Assistant have been designed to serve as the control center for our homes.

In Google's case, it allows consumers to use their voice to control smart home devices around their home that are third-party smart home products. This functionality requires specific data sharing between the connected device and the Google Assistant device to carry out a simple command.

Google is making a change in June of this year to how these integrations work which will significantly expand the breadth and frequency of data sharing and increase the rate at which data is collected and transferred to Google for their analysis.

My question to Mr. Mudd: What changes, if any, should be made to the American Data Privacy and Protection Act passed out of the committee last Congress to put consumers in control of data shared through their smart home systems?

Mr. MUDD. Thank you, Representative.

I cannot profess to be an expert in smart home data collection, but I will say that the collection of data not just online but offline certainly must be in scope for this legislation, and I am happy to get back to you with some suggestions, if helpful, on how the legislation might be improved.

I am also happy to defer to my fellow panelists here.

Mrs. LESKO. And, Ms. Rich, do you have any thoughts on that?

Also, Ms. Rich, should certain types of smart home data be subject to higher standards of privacy controls and sharing limits? For example, data about a door lock or a security system?

Ms. RICH. I would have to review the long list of sensitive information detailed in the ADPPA to see if it already captures that, but certainly when there are sensitive categories of information that might be captured by an Internet of Things technology, those should have special levels of protection.

Certainly, kids' information also should have special levels of protection.

Mrs. LESKO. Thank you.

For Ms. Givens, how do we strike the right balance between protecting consumers' data while not creating loopholes for criminals? We have had law enforcement have some concerns about the legislation.

Ms. GIVENS. Yes. So, to speak to those concerns, the bill as it stands today does not limit law enforcement's ability to pursue its investigations, to access information from companies. I understand there have been some concerns raised that by reining in the sheer extreme volume of data that data brokers are able to gather, that might impede law enforcement's ability to do kind of one-stop shopping and go to those data brokers as a source of resources for their investigations.

I would say on that point we have to reach a balance here, and when we look at the unfettered collection and the additional harms being perpetrated by data brokers, I think that that is an important balance to strike, and we need to weigh those harms.

The bill also includes some really important provisions that already consider law enforcement concerns. So, for example, users' rights to delete their information or to opt out of data brokers' information on them are limited when it might impact a law enforcement investigation. So the committee has already given careful conversation to this. I think they have landed in the right place, and it cannot be that we allow the unfettered, widespread sharing of data purposes just because of this law enforcement concern when law enforcement can still access the vital records that it needs from the first-party holders of that information, for example, credit card companies, et cetera.

Mrs. LESKO. Thank you.

Mr. Mudd, do you believe it is possible to protect personal data while also allowing businesses, especially small businesses, to efficiently digitally advertise? I mean, a number of businesses have been worried that they won't be able to advertise.

Mr. MUDD. Thank you for the question.

Yes, I do. I won't pretend that there is zero cost to business from moving to a more private approach to digital advertising, but I do believe that it will not be and should not be a catastrophic change and that the tradeoff is well worth it.

The technologies that we and others are developing, as I mentioned earlier, are employed in many other industries. They have found ways to complete what they need to do using privacy-enhancing technologies, and I think with legislation in place, we can apply the innovation that has currently been focused on extracting data from as many places as possible to instead using it in as private a way as possible.

And so my general answer to your question is, yes, I do believe it is very possible for businesses to thrive with this legislation in place.

Mrs. LESKO. Thank you.

My time has expired, and I yield back.

Mr. BILIRAKIS. I thank the gentlelady.

And I now recognize the gentlelady from Michigan, Mrs. Dingell.

Mrs. DINGELL. Thank you, Chairman Bilirakis and Ranking Member Schakowsky for holding this important hearing today and all of you for testifying.

I am hoping that this is going to be the Congress we get this done because this subject is so important. I look forward to this discussion as a continuation of this committee's very strong bipartisan work to enact comprehensive data privacy legislation.

We have got, I think, total agreement that self-regulation is not sufficient and that it has created a multibillion-dollar industry through the transfer and sell of consumer data mostly without the consent or knowledge of the consumer.

We want to empower the consumer to be the ultimate arbiter of their data while allowing companies to perform any action that consumers should reasonably expect from the use of a platform device or other technology. Any legislation that this committee supports must protect personally identifiable information, including geolocation, sensitive health data; provide what everybody has talked about today, additional protections for minors and teenagers, who to this day do not have robust protections online; minimize the necessary data captured to perform operations and promote innovation.

This topic is important and has significant ramifications on public health and safety, our economy, national security, and competitiveness. So your being here and our work really matters.

I am going to focus on data and how much is being collected and people not realizing it.

Mr. Mudd, in your testimony you mentioned the significant amount of data companies collect to develop profile of users, which I will respectfully say again nobody has any idea how much is being collected on them.

On average, how many pixels would you estimate that these companies collect on average on one individual? And are there categories of data captured that the user may not have explicitly consented to sharing while using a platform device or being tracked?

Mr. MUDD. Thank you for the question.

In terms of, you know, estimates of the prevalence of pixels and data collection, there are many out there, but, frankly, the scale of the use of these is so large that it is actually quite difficult to study them comprehensibly. I would estimate that there are well over 3 to 4 hundred, if not into the thousands of companies that are actually deploying these pixel technologies to collect data.

Now, for the average consumer, as you visit any given website, you are likely to encounter numerous of these. For a given retailer, my estimate would be somewhere on the order of 5 to 15 different pixels that are sharing data with various ad platforms. So, you know, you multiply that by the number of websites that you visit over the course of a week or month, and the ability to collect a very rich profile is certainly there.

Mrs. DINGELL. Thank you.

And, by the way, subject to misinterpretation, I always tell the committee I do a lot of my own research before committees. And I was doing opioids and within 2 hours started getting opioid drug addiction treatment ads.

I have only got a minute and 40, so I am going to ask for a yes or no from everybody on the panel. To the panel: Do you believe that, absent a national data privacy law, tech companies and others are incentivized to maximum their collection of data to participate in the digital economy and data marketplace?

Yes or no, Mr. Mudd?

Mr. MUDD. Yes.

Ms. GIVENS. Yes.

Ms. RICH. Yes.

Mrs. DINGELL. Thank you.

As we have seen at events like the Cambridge analytical scandal, data breaches present a very real threat to consumers and companies participating in the data economy.

To the panel, yes or no again: Without a national data privacy law, can companies be expected to enact stringent standards to ensure that consumers' data is secure?

Mr. MUDD. No.

Ms. RICH. No.

Ms. GIVENS. No.

Mrs. DINGELL. I got no from all three.

Last question to the panel again: Yes or no, do you believe that without a national privacy law, the amount of data that these companies acquire presents a risk to consumers and children using the platforms or devices?

Mr. MUDD. Yes.

Ms. RICH. Yes.

Ms. GIVENS. Yes.

Mrs. DINGELL. Thanks again to all of you for being here today.

Robust data protections in this space will provide safety and security for consumers' children, survivors of domestic violence, which I care about a lot, protected classes while offering businesses and industries the expectations, regulations, and the tools necessary to operate, innovate, and also, the most important thing, mitigate risk from dangerous data breaches.

Thank you to all of you for your work.

I yield back, Mr. Chairman, 10 seconds.

Mr. BILIRAKIS. I appreciate it. Thank you very much. We appreciate that. It all counts.

Next we will have Representative Pence from the State of Indiana. You are recognized for 5 minutes, sir.

Mr. PENCE. Thank you, Chairman. Thank you for holding this meeting.

Thank you to the witnesses for being here today.

You know, you are hearing the same thing from everybody because we all feel the same way. Our constituents all feel the same way. I can tell you feel the same, the data privacy.

And, Ms. Givens, when you said that we have had 21 hearings in 5 years, I took all of my comments and I threw them out because I thought, well, here we go again. It is almost like we are just déjà vu, doing the same thing over and over and over.

And Mr. Mudd, in your testimony, which with Ms. Dingell you were making this point again, and I am going to quote, "the scale of data collection and transfer using these mechanisms is difficult

to comprehend how big, how much data you are collecting from me.”

I walked in this morning, and I have a letter from Privacy for America. I don’t know anything about them, really, but here they say that consumers’ incomes have been enhanced to the tune of \$30,000 because of all of this data collection. And I think that is great.

So my question gets to the money. I have been a businessman all my life, and if data collectors—and they are sitting in this room—are providing me \$30,000 in services, how much are they making to give me that much value?

And since it is incomprehensible the amount of data being taken from me, and I am going to ask you each of this, can I be compensated for this incomprehensible amount of data that is being taken from me?

Starting with you, Mr. Mudd.

Mr. MUDD. Sure. Thank you for the question.

Whether users can be directly compensated or not I think certainly is an interesting question, one that has been posed many times in the past and should be further explored.

I will say that the notion that the only way that businesses can leverage digital advertising effectively is through this incomprehensible collection of data is absolutely false and that there are other ways through this problem that do not sacrifice the privacy of individuals and that those technologies, as I have mentioned earlier, are employed elsewhere in a proven fashion.

Mr. PENCE. You know, if I can go off on that, I have done a lot of digital advertising in business, OK? And we have thrown out the baby with the bath water when it comes to mail, radio, and TV. And I am not doing an advertisement for the other mediums or the other venues, OK? But I have found that digital advertising for a small business is not very effective.

But back to the same question. Can I make money off my data that everybody has taken from me?

Ms. GIVENS. Like my colleague, I will say it is an interesting question, but I don’t think it gets to the heart of how we protect consumers going forward. But discussions about monetization and compensating users doesn’t actually get them the protections they—

Mr. PENCE. OK. I can see where you are going with that, Ms. Givens, but if 21 committee hearings in 5 years isn’t moving the ball forward and in a sense there is almost a sense of delay, keep talking about the same thing, why wouldn’t finding a way to monetize, for me to get paid for my information, why wouldn’t that maybe change the trajectory?

Ms. GIVENS. Well, it is my job to be an optimist, and I think this committee has made progress as a result of those 31 hearings, and we are close.

But what is important and I think what needs to be addressed here is that really, in the advertising world, we have market failure. Right now the only incentive is a race to the bottom, to hypertarget as much as you can.

And for the digital advertising companies that offer the most specific profiles on people, they are the ones that win the race, and

there is no incentive for them to innovate into privacy-protecting ways of delivering ads that matter. That is the innovation we want to encourage.

Mr. PENCE. Thank you.

And I will move on to the last witness.

You know, if I get to opt in because I will get paid for it, maybe that will change their behavior too.

OK. And then, finally, last witness?

Ms. RICH. Oh, you are asking me?

Mr. PENCE. Yes, ma'am.

Ms. RICH. You are asking me the same question?

Mr. PENCE. Yes, Ms. Rich.

Ms. RICH. Well, one of the problems with that idea of an even exchange is that it hasn't worked in terms of notice and choice where consumers have to individually, you know, supposedly negotiate with each company. So I think it is putting the burden—

Mr. PENCE. Well, I was in the banking industry, and we had truth in lending where you had to make it real simple what you were agreeing to when you clicked "yes."

But, with that, I have run out of time. Mr. Chair, I yield back.

Mr. BILIRAKIS. I appreciate that very much.

Now we will have the gentlelady, my good friend from the Tampa Bay area, Representative Castor. We will recognize her for her 5 minutes.

Ms. CASTOR. Well, thank you, Mr. Chairman and my good friend. And thanks to the ranking member.

And, to the witnesses, thank you. You have been very strong and have provided very clear expert advice to the committee. We need it.

This is really our kick start to our privacy effort this session, and it is heartening to understand that it is a priority for us across the aisle here.

I was very proud to contribute to the committee's efforts in the last Congress for the American Data Privacy and Protection Act, particularly the provisions relating to children's online safety, because ADPPA included elements of my Kids PRIVCY, such as the targeted advertising ban, age-appropriate design provisions, enhanced limitation on sharing children's personal information with third parties, special protections for personally identifiable information about children, a dedicated Youth and Privacy in Marketing Division at the FTC, and increased oversight of COPPA safe harbors.

I really urge my colleagues to act with urgency here. The harms to kids online are now very clear, and we really shouldn't take too much longer to act. We need to do this for all Americans, but I think there is a special threat to children's online privacy and safety.

The Children's Online Privacy Protection Act, COPPA, is wholly outdated. It has been many years since the Congress has acted. Can you all take a look at that, at what has happened since the adoption of COPPA, and give us some examples of what you see as a growing online harm to children and all Americans?

Ms. RICH. Well, for one thing, COPPA is limited to children under 13, and as this committee and other work done in other com-

mittees has shown, there were a lot of harms at least to people who are, you know, under 16 or 17. You could go higher too, but all the things we have seen with social media. So, if this committee and the public is seeking greater protections for teens, COPPA doesn't do it.

COPPA also is very basic, and the FTC, even in the 2013 rule review, which was the last one, did summersaults to try to get at the platforms, to try to protect information that wasn't listed in the original COPPA statute, like location data and IP addresses. And so it absolutely needs to be updated to reflect what has happened since COPPA was passed in 1998.

Ms. CASTOR. And you highlighted the fact that the FTC hasn't been using some of its tools. Now, in response to language I offered in the fiscal year 2022 omnibus, the FTC published a report providing details about its work on COPPA. In that report, the FTC stated that the Commission dedicates approximately 9 to 11 staff and has opened 80 investigations of potential COPPA violations in the past 5 years.

That is woefully inadequate, and even the FTC says as much in the conclusion of their report. They stated: "With more resources, however, the FTC could do more."

And we need them to do more.

Do you think the FTC should have more resources and authority to protect kids online?

Ms. RICH. Absolutely. It is shocking how few resources the FTC has for privacy. It is a fairly large proportion of the consumer protection mission, but it is about 50 dedicated people to privacy, which if you consider that to other countries that are much smaller and the kind of staff they have to police privacy, it is just woefully inadequate. The FTC absolutely needs more resources, but it also needs more authority because the authority is thin.

Ms. CASTOR. Ms. Givens?

Ms. GIVENS. The one point I would add on the FTC resources is that all of the research shows that it is an excellent investment of taxpayer dollars. The Congressional Budget Office has shown that for every dollar invested in the FTC, taxpayers get \$3 in return because of the enforcement power that it would add to the agency.

So I think it is incredibly important when we think not only about protecting consumers but good governance as well.

Ms. CASTOR. I want to thank—my time is running out. I want to be sure that I take time to thank Ranking Member Schakowsky for being a leader on giving the FTC more resources to protect consumers, and I hope we will continue this Congress.

And I want to thank the chair, Mrs. McMorris Rodgers. I heard her clarion call at the beginning of this hearing loud and clear, and I appreciate her outreach to my office, and we are going to continue working to make ADPPA strong for all consumers, especially our kids.

Thanks. I yield back.

Mr. BILIRAKIS. I thank the gentlelady.

Now I recognize the gentleman from the State of Georgia. Mr. Allen, you are recognized for 5 minutes, sir.

Mr. ALLEN. Thank you, Mr. Chairman and Ranking Member, for holding this hearing on the need for a national privacy standard.

I think today we are getting closer than ever to enacting some type of nationwide privacy and data security framework, which will give businesses the certainty they need to innovate while providing Americans more control over their data.

I appreciate the hard work done by Chair Rodgers and Ranking Member Pallone last Congress to get to this point, and I look forward in engaging and getting this done in this Congress.

Mr. Mudd, as a former employee of Meta and now as chief product officer of Anonym, you have seen both sides of the advertising ecosystem. Kind of help us understand exactly how they make the money that they make in using our information.

Mr. MUDD. Certainly.

So the collection of data I described earlier, you know, it is based on your behavior on websites and often is then shared with the ad platform that any given advertiser is using to find their customers.

Now, how do those ad platforms make money using that data? I think that was your question.

Well, effectively, the better the ads work, that is, the more effective they are in identifying specific individuals who are likely to be customers of any given company, the more those ad platforms can charge for those ads. And so their incentive, of course, is to improve the relevance of the advertising. Nothing wrong with that incentive in and of itself. It is the means by which they do it that we have talked about that is oftentimes very problematic.

And so that incentive challenge—gather more data to become more relevant in order to charge higher prices for ads—is at really the heart of the vicious cycle that we are faced with today.

Mr. ALLEN. Yes, and as I see it, there is certain information that, obviously, I just want maybe me and my family to know about me, and they like to get that information. Does it bring the highest price?

Mr. MUDD. It is a good question. You know, the value of data, you know, is certainly, you know, variable based on who the advertiser is, right. Location data is very important to an offline retailer who wants to find customers that are near their outlet whereas healthcare data is very valuable to different types of advertisers.

Mr. ALLEN. What role do the data brokers play in this?

Mr. MUDD. Data brokers oftentimes enrich, as the term of art is called, the profiles of ad platforms that might not be able to collect that information themselves.

So to give an example, maybe a newspaper site doesn't have any real insight into, you know, your financial history and so forth, but they would love to be able to sell advertising to credit card companies. And so they go to the data broker, buy that data about your financial situation, and therefore can sell to a credit card company more effective advertising.

Mr. ALLEN. And any idea how much this information is being held and used by data brokers?

Mr. MUDD. I don't know that I could find a way to quantify that for you. All I can say, as I said earlier, is that it is incomprehensible to any ordinary citizen, and the scale is quite massive.

Mr. ALLEN. Well, you know, my State has been ranked as the number-one State to do business in, in the last 10 years, and in my

younger days I started a company, a small business, and I was a small business owner until I was elected to Congress.

I know a lot of small companies can unintentionally bear the brunt of regulations if protections aren't carefully crafted. How can companies like yours enable small businesses without sacrificing the privacy of consumers?

Mr. MUDD. Thank you for the question.

I think there are a number of ways. First of all, I would say that we want to encourage competition in the digital advertising ecosystem, and to do that, what we need to do is level the playing field so that smaller publishers and ad platforms can compete with the largest ones more effectively.

By enacting legislation like ADPPA, we take a meaningful step forward in making the digital advertising ecosystem, I believe, more competitive, which will serve small businesses in providing them more options for promoting their business, you know, and competing with larger businesses.

Mr. ALLEN. And, Ms. Rich, I have got 21 seconds, but why is it essential that any data privacy law protect all Americans regardless of age?

Ms. RICH. Because all Americans, regardless of age, need privacy protections and haven't had it.

And, by the way, it hasn't been 31 hearings. It has probably been several hundred since I have been participating in this debate.

In addition to the kids' provisions, though, the ADPPA would provide—not only would it provide targeted protections for kids of the kind that we have already talked about, but even the adult, even the general provisions—data minimization, data security, privacy by design—would also protect kids, which is why we need to do it all together.

Mr. ALLEN. Thank you.

And I yield back.

Mr. BILIRAKIS. Thank you very much. I appreciate it.

Now I will recognize Ms. Clarke from the State of New York for her 5 minutes of questioning. Thank you.

Ms. CLARKE. I thank you very much, Mr. Chairman, and I thank our Ranking Member Schakowsky for holding this very important hearing.

I also want to thank our witnesses for testifying here today. You have really enriched the debate and conversation in this space.

I was encouraged that major pieces of my bill, the Algorithmic Accountability Act, were included in the ADPPA that this committee marked up last year. I hope to continue working with Members on this committee to ensure any national data privacy standard requires algorithmic transparency and risk mitigation.

AI systems are often trained on the datasets that replicate human biases, and, thus, bias is built into the technology itself. I am concerned that, without proper transparency and explicit steps to mitigate against bias, the use of artificial intelligence and critical decisions could erode essential civil rights protections in the digital realm.

Discrimination, whether done by a person or an algorithm, cannot and must not be tolerated.

Ms. Givens, in your testimony, you highlighted how AI and automated decisionmaking is already used in a wide range of decisions like employment, lending, and tenant screening. Could you elaborate on why requiring transparency with algorithmic use and algorithmic impact assessments are a critical part of comprehensive consumer data privacy legislation?

Ms. GIVENS. I can. And I have to start by thanking you for your incredible leadership on these issues over the past few years, really shining a light on these concerns and how we can move forward to address them.

Tools that use algorithmic decisionmaking are increasingly being used in ways that significantly impact people's lives. To give just one example in the employment context, we are seeing the increasing use of vendor-created tools to screen résumés, to conduct video-based interviews and analyze those interviews, to have people play online games.

And the way in which these are AI-driven is that those tests are automatically looking for traits that match the traits of existing people in the company, which is an automatic recipe for perpetuating existing systems of discrimination and also raise questions about fitness for purpose in the first place. Are you actually measuring things that really are indicative of someone's likelihood to succeed on the job?

And there has been important research done in the field to show that often these tools actually are not fit for purpose. One of the most notorious examples analyzed an AI resume tool where there was weighted factors in favor of a candidate if their name was Jared and if they had played lacrosse in either high school or college.

The reason this matters is not just for the employees who are being screened out but also for the businesses that are relying on these tools based on commitments from vendors that they have been screened, that they are appropriately designed, and they are bias-free.

How can businesses actually trust that these tools are doing what the vendors say they do and that they are complying with existing law?

So transparency really matters, and what ADPPA does, lifting many of the important provisions from your legislation on this issue, is say we need to have companies, number one, disclose how these tools work, what data they are based on, do it in a way that protects trade secrets and doesn't overwhelm but analyze this, and the company's need to show they have gone through a rigorous internal process of detecting potential bias and assessing fitness for purpose.

The reason that matters is that we need to inculcate a company culture of asking those questions before we put these tools out into the world, and that is what ADPPA will help do.

Ms. CLARKE. Well, thank you. As a member of the Committee on Homeland Security, I am particularly concerned with what can happen when companies collecting our sensitive information are not adequately protecting that information.

Ms. Givens, if companies are largely free to collect, possess, and transfer user data that is not necessary to provide a specific prod-

uct or service, does that increase the risk or a consequence of a data breach?

Ms. GIVENS. It does absolutely, because without those purpose limitations or minimization requirements, it leads to the unfettered sharing of additional information solely for the purposes of helping to target ads, and that is what leads to these massive data sets that can be so vulnerable to abuse.

Ms. CLARKE. Thank you.

Ms. Rich, how would you—how would a comprehensive national policy framework increase the FTC's ability to protect the American public from data breaches?

Ms. RICH. Oh, there are so many ways. First of all, there are the data security provisions in the order that would require data security to protect the data, but also many of the core provisions would serve the same function—data minimization. So many data breaches happen to data that is sitting there and shouldn't be. And same with protections for sensitive information. If people can prevent their sensitive information from being overcollected and stored, it is less likely to be breached.

So there are so many ways in which this helps the FTC and, you know, not even—in addition to giving them civil penalty authority, which they do not have for first-time violators to increase deterrence.

Ms. CLARKE. Mr. Chairman, I thank you, and I yield back.

Mr. BILIRAKIS. Thank you so very much.

OK. Now what we will do is we have votes on the floor, and we will recess and come back 10 minutes after the final vote, because I have several Members on our side, on the Republican side, that haven't had the opportunity to ask questions, whether it is sitting on the committee, but we have had several that have waived on as well. And I really think we need to give them an opportunity.

I appreciate the witnesses for their patience. Thank you so much.

So we will go ahead and—without objection, we will recess.

[Recess.]

Mr. BILIRAKIS. All right. The meeting will come to order.

I want to thank y'all. I thank the witnesses. Y'all were outstanding, by the way, OK, and the consensus is really good for us to know that we—I mean, we knew it anyhow, but to know that we passed a good bill last session and we can improve upon it, and y'all are contributing factors, there is no question.

So why don't I recognize my good friend from east Tennessee, Ms. Harshbarger, who is our—what is it, the—yes, the youngest pharmacist.

Mrs. HARSHBARGER. Yes.

Mr. BILIRAKIS. The youngest pharmacist on the committee.

Mrs. HARSHBARGER. Youngest. Buddy can still claim the oldest.

Mr. BILIRAKIS. Recognize you for 5 minutes.

Mrs. HARSHBARGER. Thank you, sir. Thank you, Mr. Chairman. Thank you for the witnesses.

My first question, sir, is for Mr. Mudd. One of the reasons that America has such a robust economy is because startups are able to establish themselves in the marketplace. What safeguards should authors of the Federal privacy legislation build in specifically for the protection of the small and medium-sized businesses?

Mr. MUDD. Thank you for the question. You know, I do believe, and I am no expert, that there are some provisions that safeguard the, you know, smaller businesses and their use of data, and I think those are very much appropriate. I would say that it is—it is important to level the playing field between smaller companies that are trying to establish a publishing presence and an advertising business online and the very large ones. And I think this bill goes a long way towards leveling that playing field and raising the bar across the board so that it is not just the largest tech companies that have access to the data that is so powerful in advertising business and that have such an incumbent advantage.

Mrs. HARSHBARGER. OK. Very good. That kind of leads me into my next question. You know, I am thrilled we are working to draft a privacy framework that appropriately balances data privacy for our constituents while also helping businesses receive more clarity about the rules of the road. Black-and-white clarity of what is and isn't permissible is especially important for these small and medium-sized businesses who don't have dedicated compliance departments and lack the resources to survive endless lawsuits from predatory attorneys.

And I can say that because I have been a small business owner of independent pharmacies for over 30 years, and, believe me, I know that it is incredibly difficult to navigate the rules, the privacy rules, the data rules, the healthcare rules, from State to State. And then you have to outsource that to be compliant to somebody who knows the rules and, therefore, you run the risk of having that data compromised and used. You know, healthcare fraud is very prevalent, as you mentioned.

My question is: What can be done to ensure there is clarity for all these businesses to thrive under a Federal privacy framework? And I will open that up to all three of you, whoever wants to go first.

Mr. MUDD. I will mention one thing and then I will pass it to my colleagues here, and that is just that I think a State-by-State patchwork is particularly onerous to small businesses who are trying to comply with different rules, as you mentioned, and that even just establishing a single benchmark and compliance program would go a long way toward supporting small business and innovation.

Ms. GIVENS. In addition, the ADPPA has a number of protections to help small businesses. So some provisions don't apply to small businesses or they have a lesser burden. For example, access rights for users to access and understand the data that is held about them, and the private right of action as well. So small businesses are shielded from that.

In addition, there are provisions like making sure the FTC provides a business resource center to help businesses actually comply and understand their obligations, which is really important, as well as some of the other provisions to address these concerns about excessive litigation or runaway litigation. There are limits on the damages provisions that can be sought. There is this notice and cure opportunity that the Chair was talking about. So other more measures to make sure the consumers can vindicate their rights,

which is so important and what Congress is focused on, while also making sure that businesses aren't overly burdened.

Mrs. HARSHBARGER. OK. Very good.

Ms. RICH. I would add one thing to what my splendid copanelists have just said, which is what we discussed with Chair Bilirakis, which is the compliance programs. If you have a rigorous compliance program and small and medium businesses can join and get some certainty and help in their compliance, it benefits everybody.

Mrs. HARSHBARGER. Exactly. I keyed in on that point when you were talking previously.

I guess another question—and this will be to each one of you too—can you think of an example of an unintended consequence with a Federal privacy legislation?

And I say that because, you know, when you poll this across the country, across businesses, across citizens, they want one policy so it is easy to navigate. But would there be any unintended consequences for businesses or individuals?

Ms. GIVENS. So I will chime in that States have a really important and legitimate role in protecting their citizens, and we need to make sure that at the same time it is fighting for consistency for businesses and how they think about consumer privacy. We are not infringing on States' rights to protect their citizens and the values that they care about. And thinking about things like consumer protection laws of general applicability, civil rights laws.

A number of States have been really important first movers on things like child exploitation online, antispam laws, data breach notification laws which are in place in all States around the country. And people have gotten used to those. They have been on the books for a long time, and States have played a really important role. So we need to strike a balance here of creating that certainty for businesses but still allowing the States to provide that traditional function they have had of protecting their citizens, and that is the balance the ADPPA is trying to strike.

Mrs. HARSHBARGER. Anybody else?

Ms. RICH. I will just quickly add research. We need to incentivize research using data, and the ADPPA does it while also having protections. So that is very important.

Mrs. HARSHBARGER. Yes, ma'am. I agree. Well, with that—go ahead, sir.

Mr. MUDD. Oh, the only thing I would add to that is I do think a potential unintended consequence of a privacy law is to constrain, you know, unnecessarily at least, the use of data for very productive reasons by small businesses. And so I think technology, again, can really help to bridge that gap, but it would be all the more helpful if, to the degree possible, the law is very clear about what does constitute reasonable privacy and what doesn't, so that technology companies know how to, you know, sort of navigate the solution.

Mrs. HARSHBARGER. Absolutely. That goes back to clarity.

Mr. MUDD. That is right.

Mrs. HARSHBARGER. Thank you. And, with that, I yield back, sir.

Mr. BILIRAKIS. Thank you. The gentlelady yields back.

No one on Democrat side, so we will recognize the gentlelady that represents Gator Nation, Ms. Cammack, who is a great friend of mine.

Mrs. CAMMACK. Thank you, Mr. Chairman. And, yes, we do represent the Gator Nation, home to one of the best damn football teams in all of the Nation, as well as a wonderful research institution.

So, Mr. Chairman, thank you for your support, not just of the Gator Nation but of this issue. I think it is critically important that we address this issue, and I feel like we have hit on all of the topics really in some way or another.

So I do want to give you all the opportunity to narrow in on something that hasn't been addressed here yet today. But before I do, while you are thinking of that, I would like to ask you guys, particularly when we are seeing Federal agencies collect data from various companies and then using that data in ways that may or may not—I am not going to say ethical, but there is a bit of a gray area in how that data is being used, what are some of the national security implications for that data collection and then the subsequent breaches that we have seen?

And I will start with you, Ms. Rich, and then we will go down the line.

Ms. RICH. Well, there are so many ways this has international implications. That is a big piece of this. For one thing—well—for one thing, you know, U.S. companies are having serious problems in Europe because Europe believes that the U.S. doesn't have strong enough laws. It affects trade. It affects companies' ability to process European data. And then, in the U.S., because they are not allowed to transfer it, which creates a lot of inefficiencies. So that is a serious trade and credibility issue we have.

As we deal with issues of hacking and surveillance from other countries, there is—not only is the data exposed, but we have very little credibility as we deal with those other countries. And, you know, it comes up, you know, in the TikTok situation, people talking about banning TikTok. Well, I think we would have more credibility talking about that if we had a privacy law of our own. And then there's the costs of disproportionate costs on U.S. companies of complying with multiple laws.

Mrs. CAMMACK. And I appreciate it. I want to make sure to give Ms. Givens and Mr. Mudd an opportunity as well, as quickly as you can.

Ms. GIVENS. So I agree with my colleague, and I do think the biggest risk to all of this is the unfettered collection, storage, and sharing of data. And that creates cybersecurity risks. It creates national security risks. And so that is why we have to pursue a framework that minimizes the amount of data that companies are collecting and storing and puts limits on how they can share that information.

Mrs. CAMMACK. Mr. Mudd?

Mr. MUDD. Very much agree with that. And, you know, in the tech world, we call that surface area, right? The more the data is out there, the bigger the risk, right? Data is intimately replicable and can be stored, you know, forever. And so to the degree that we

are able to limit it through technology, through regulation, then we reduce the risk, national security and otherwise.

Mrs. CAMMACK. Do you think that we should require or have a way to incentivize that data servers be housed here in the United States as part of the national security framework when we are talking about housing our data, Ms. Givens?

Ms. GIVENS. I think that gets you into risky territory really quickly, and part of the reason is we need the global flow of information around the world. It is how the global internet functions. It is how we are able to communicate and do business with other nations. It is the way in which the U.S. is being a leader, and innovation around the world is through that free flow of information.

So instead of just throwing up firewalls, what we need is strong data protections across the board to make sure that everyone is following the same rules, as opposed to having to impose these really hard-to-enforce laws on data localization.

Mrs. CAMMACK. Something that I haven't heard yet today is the emergence of AI, ChatGPT, how AI is going to essentially revolutionize the data collection models, and what are some of the implications of using AI with some of these algorithms and these platforms? We can go down the line, and then I will open it to you in the 1 minute and 7 seconds that I have left.

Ms. Rich.

Ms. RICH. One implication is this is an area where technology has become so sophisticated, and the FTC laws, basic laws, can't get at it in the way they were able to get at issues earlier.

Mrs. CAMMACK. Thank you.

Ms. GIVENS. Congress is going to be grappling with this issue for a long time as AI transforms our society. One of the first things we need to do is just get a handle on which companies are using these tools and making sure that they are going through a responsible process when they are deciding how to design them and how to deploy them to impact assessments. And that is one of the provisions in the ADPPA and why it matters.

Mrs. CAMMACK. Excellent. Thank you.

Mr. Mudd.

Mr. MUDD. Would make two points. First, that regulating the use is really important, as Ms. Rich mentioned, and flexibility to adapt, you know, to further use cases along the way is really important. The second is I think that explicit bias detection can play a really meaningful role in this. And then the last would just be around transparency, right, understanding when AI is used and so consumers have some understanding of the end result.

Mrs. CAMMACK. Excellent. My time has expired, so I will have to yield back, so sorry.

Mr. BILIRAKIS. I thank the gentlelady.

Mrs. CAMMACK. Maybe Mr. Obernolte will give you a few moments. Thank you.

I yield back.

Mr. BILIRAKIS. OK. Very good. Now we will recognize—there is no Democrat. They are all getting ready for their issues conference. So we are going to go with Representative Armstrong, the vice chair of the full committee, from the great State of North Dakota.

You are recognized for 5 minutes.

Mr. ARMSTRONG. Thank you, Mr. Chairman.

And before we had to recess, Ms. Givens, you had an interaction with Congresswoman Lesko, and you talked about the balance of law enforcement and primary source versus secondary source data. I think it is important to point out the biggest difference, at least in most cases, between secondary source data and primary source data: One requires a warrant, one doesn't. And I personally think the privacy portion of this is a feature, not a buck.

Are you familiar with the September 26, 2022, letter to the House from various law enforcement associations expressing concern with potential data privacy legislation? There is a quote that it has major negative consequences that would make it harder to investigate criminal activity.

Ms. GIVENS. Not the specifics of that letter, but I am with the general set of issues raised.

Mr. ARMSTRONG. Well, the letter continues and it says: "will likely complicate the private sector's ability to continue its ongoing efforts to cooperate and voluntarily share certain information with law enforcement."

Essentially, the letter addresses the warrantless purchase of consumer data from brokers to generate investigatory leads.

Are you familiar with the Center for Democracy and Technology report from December of 2021?

Ms. GIVENS. I am. My team and colleagues wrote it.

Mr. ARMSTRONG. "Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers."

Would you mind briefly summarizing the general conclusion of that document?

I will let you weigh in too, Mr. Mudd, because you have been pretty fired up about some of this stuff.

Ms. GIVENS. So yes, one of the major concerns about data brokers is that they aggregate these vast amounts of information. And in addition to selling it to target ads, it does become a target for law enforcement. And law enforcement is able to buy that data on the open market, like any other person, and in doing so circumvent their Fourth Amendment obligations.

So CDT and other civil society organizations have been vocal in raising the constitutional concerns that that raises and the protections for people's freedoms and civil liberties. We are not saying that law enforcement work shouldn't happen—of course it should—but it needs to be subject to reasonable oversight in the constraints of the Constitution and the law.

Mr. ARMSTRONG. Well, I want to be perfectly clear. Law enforcement should use every tool. Good law enforcement officers are going to use every single tool that exists for them to solve crimes, to do all of those things. It is our job to set the guardrails on this, and it is the Federal Government's job to set the guardrails on this, because it actually implicates what I think is maybe the most existential conversation of the 21st century and what the actual right to privacy means as we continue to move forward.

The report cites DOJ's use of commercially aggregated data for prosecutions related to January 6th. Grand jury information states

location data history for thousands of devices were present inside the Capitol, were essentially obtained from several sources.

I was at the Capitol that day. I was performing a constitutionally and statutory mandated function. You think DOJ had access to my data?

Ms. GIVENS. Sir, I wouldn't want to speculate on a particular fact pattern, but—

Mr. ARMSTRONG. I think they did, so—Ms. Givens, hundreds of journalists were at the Capitol that day. They were performing activities expressly protected by the First Amendment. And you wouldn't want to speculate, but that information existed as well. And I am more than willing to guess that locator systems and toll records were collected from around the beltway. There are lots of other commercially available data that was probably accessed.

Mr. Mudd, are you familiar with the majority in *U.S. v. Carpenter*?

Mr. MUDD. I am not.

Mr. ARMSTRONG. OK. Ms. Rich, are you?

Ms. RICH. Yes.

Mr. ARMSTRONG. So the time-stamped data referring to cell site location information provides an intimate window into a person's life, revealing familial, political, professional, religious, and sexual associations. And I think the court has—this particular court, and even the previous iteration of the court, has been willing to reexamine what privacy looks like in the form of the government in the digital age. And we have talked a lot about data collection and data brokers. And I think I will just be more blunt really quickly.

Data brokers say this will put them out of business, which means not only will law enforcement not have access to this, but other people won't. But I think we don't spend enough time talking about—I mean, data collection is just the first part. Representative Cammack just talked about AI, talked about all this. The ability to analyze that data in real time is advancing at an incredibly rapid rate, which makes it very much different than having a drug dog search a box at a post office.

And how do we deal with this and continue towards constitutionally protected activity when the Federal Government has what I think is an incred—all law enforcement has this end run around the Fourth Amendment by being able to purchase this data on the civilian market?

Ms. RICH. That is exactly right. If our rights exist for a certain reason, you shouldn't be able to just go to another company and get the same data and not abide by those rights. It is an end run. That is exactly what it is.

Mr. ARMSTRONG. With that, I will yield back. And I apologize to Mr. Mudd. I kind of wasn't totally honest with him.

Mr. BILIRAKIS. Thank you. The gentleman yields back.

No one on the Democratic side. So we will recognize Representative Fulcher for his 5 minutes, from the great State of—right, Idaho?

Mr. FULCHER. Idaho, yes. Thank you, Mr. Chairman.

And to our panelists, thank you for your participation today and for your testimonies. And as I have said in previous sessions, please understand that some of us have dueling responsibilities,

and so the fact that we are not here the entire time doesn't mean we don't care what you have to say. To the contrary, very much so, and for your written testimony as well.

I want to focus on two things, and I am going to ask Ms. Rich to start this, please. Transparency and algorithms and what those relay, what those do is something I am very interested in. I think that there needs to be some exposing of that and some increased improved transparency.

My question for you: Is it possible to have transparency without exposing secrets necessary to operate a business?

Ms. RICH. Are you referring to the algorithms?

Mr. FULCHER. I am referring to the algorithms used.

Ms. RICH. Yes. Assessments. Yes.

Mr. FULCHER. Yes. And expand on that if you would, please.

Ms. RICH. So the FTC can seek a lot of information right now that would be used to create those assessments. The assessments, though, create even more transparency so that an agency can look to see if laws are being violated and being adhered to. The FTC already has a model for this, because in all of its data security orders and its investigations too, it gets very, very sensitive information and even audits in those orders, which it evaluates. So it can do this, and there are procedures for protecting trade secrets and keeping the confidential information in those reports private. There's extensive confidentiality procedures.

Mr. FULCHER. If I could ask you to take that same analysis and direct it towards, what about the end user of that information, of that—you are talking about the FTC, I think.

Ms. RICH. Yes.

Mr. FULCHER. What about for the transparency by the user?

Ms. RICH. I think that is more difficult because I am not sure that consumers are really going to understand all the details disclosed about algorithms. The information that the FTC gets is probably pretty complex and they need technologists to help them evaluate it and figure out whether discrimination is going on. So while there could be some mechanisms for explaining the algorithms to consumers, I am not sure we would want to give it to them. I don't think it would mean much, and it would be very difficult then to protect it.

Mr. FULCHER. My personal concern is the use of the data, who owns that data, how that data gets used. Mr. Mudd has talked about that. I caught a piece of that. I am going to do a followup question with him. But that is—this is a big, complicated issue.

And so one followup to you, if I may. Is the FTC the best entity to be the regulator of that, the monitor of that?

Ms. RICH. Yes, it is the most experienced, but it would need to get help. It needs more technologists. It needs more resources if it is going to be evaluating algorithms.

Mr. FULCHER. Statutory changes as well?

Ms. RICH. Excuse me?

Mr. FULCHER. Statutory changes as well?

Ms. RICH. It totally needs statutory changes. It needs the ADPPA or something like it.

Mr. FULCHER. OK.

Ms. GIVENS. Mr. Fulcher, if I may, there are provisions in the ADPPA that protect trade secrets. And so the vision is that those impact assessments are performed by companies, submitted to the FTC, that can then look further into them if they want to. Disclosure to the public is optional by a company, and there is specific language in there to protect trade secrets while still making sure companies are going through that assessment process of really making sure they are being honest and thoughtful about the—

Mr. FULCHER. In your opinion, is that language sufficient?

Ms. GIVENS. Yes, I think it is well drafted.

Mr. FULCHER. All right. Thank you.

Mr. Mudd, shifting gears a little bit. I want to talk about GDPR. Maybe I am not shifting gears all that much.

My perception of what has transpired in Europe over that is that it has been helpful to large companies, not so helpful to small companies.

First of all, is that your perception as well? And secondly—we have only got about 50 seconds left—is, what is the primary component or components that need to be different when we embark on that path?

Mr. MUDD. Sure. My perception matches yours, that it has likely been more—easier for larger business to adjust to that regulation and to comply with it, and therefore probably more difficult for smaller businesses.

In terms of what we got to learn from GDPR and potentially do differently, I think one of the challenges with GDPR, putting my sort of consumer hat on, is that it really does put a lot of work on the consumer to read and understand many, many, many consent dialogues. And instead, I would hope that we can find a way to sort of raise the bar, as we have talked about, instead of asking consumers to navigate very difficult choices, in some cases no choice at all, if they want to access content.

Mr. FULCHER. So the answer is get rid of the complexity?

Mr. MUDD. I think reduce complexity, but more importantly focus on data minimization and technologies that support that, as opposed to asking consumers to say yes or no to answers they have very little understanding of.

Mr. FULCHER. OK. Thank you.

Mr. Chairman, I yield back.

Mr. BILIRAKIS. Thank you very much. I appreciate that.

Now we will recognize—he waived onto the committee, appreciate it, one of the hardest workers in Congress. I am not even going to mention the pharmacy thing. It has been overblown.

Mr. CARTER. Thank you.

Mr. BILIRAKIS. Yes, I am not going to do that. But in any case, I will yield 5 minutes to my friend from the State of Georgia.

Mr. CARTER. Thank you, Mr. Chairman, and thank you for having this hearing.

And thank y'all for being here. As was indicated, I am pharmacist. I am not an IT technician, but I will tell you I am a consumer, and I am concerned. And, you know, I have experienced it myself. I have experienced—I have a truck. I have got a Toyota Tundra, 478,000 miles on it, and I am going to get to 500, I am sure.

But, you know, I had a cover on the back and it dry-rotted, and I needed to get a replacement for it. And I just searched for it, and then all of a sudden, I started getting all these ads for this. And I thought, how in the world? So it is real. This is real, and this is something—and this is why I wanted to waive on, because this is so vitally important to us. And it is just fascinating to me because I know we need to do something, but I want to do the right thing. I don't want to suppress freedom of speech. I don't want to suppress innovation. But when you don't do something, you are doing something. And if we don't do something, then we are going to be in a mess.

Mr. Chairman, to begin with, according to the Information Technology and Innovation Foundation, over the next 10 years, it is estimated that the growing patchwork of State privacy laws that we are experiencing will cost over a trillion dollars, with at least \$200 billion hitting small businesses. And I know about small businesses because I ran one for 32 years. So I am—I do have some expertise there.

But, Mr. Chairman, I would like to ask unanimous consent to include this report from the ITIF in the record.

Mr. BILIRAKIS. Without objection, so ordered.¹

Mr. CARTER. OK. Ms. Rich, I want to start with you and get right to it. Mr. Bilirakis hit on this earlier in the hearing, but the FTC rulemaking won't be preempting the five States with the enacted laws, nor any succeeding legislation. So I agree with you, we—this committee, we have the responsibility to pass a national standard, and that is going to be extremely important.

But I want to dig into the FTC rulemaking a little bit more. I understand there is a difference between the FTC's APA rulemaking authority and their Mag-Moss rulemaking authority. I have heard there may not be legal authority for the FTC to do their own privacy rule under Mag-Moss, but their authority is pretty clear cut.

Can you put on your FTC expertise hat right now and give us your thoughts on whether they have a legal standing to promulgate this rule?

Ms. RICH. Yes. And thanks for the question. So the FTC Act explicitly authorizes the FTC to develop rules under this so-called Mag-Moss process to hold and remedy unfair deceptive practices. It even tells the FTC what process to use. And the FTC has used Mag-Moss to develop other rules. So I think the FTC is on pretty solid ground, generally, doing rulemaking using this tool. The problem is it is very cumbersome, and it is limited so that, you know, given the breadth and significance of the privacy issues here, the FTC may not—can't do so much of what is in the law that you guys have been, you know, writing and grappling with.

Mr. CARTER. Absolutely. Absolutely. Even more reason why we need to pass a national standard.

Ms. RICH. Yes.

Mr. CARTER. Mr. Mudd, I want to go to you. In your opinion, do you think overly restrictive rules that stymie innovation—because

¹The information has been retained in committee files and is available at <https://docs.house.gov/meetings/IF/IF17/20230301/115376/HHRG-118-IF17-20230301-SD021.pdf>.

I am concerned about freedom of speech. I am concerned about stymieing innovation as well. I don't want to do that. The internet is one of the greatest inventions of our lifetime. I get it. And I understand that, but at the same time, as I said earlier, if we don't do something, you are doing something. You know, we have got to address this. And it is incumbent upon us, us here in Congress. That is our responsibility, and we are responsible people. I know that some people would disagree with that, but I don't. We are. We need to do something.

But just let me ask you, do you think that overly restrictive rules that would stymie innovation and the data-driven economy harm America's competitiveness with respect to our global competitors?

Mr. MUDD. I think there is potential, but I don't believe the ADPPA will have that effect. I believe that what technology companies big and small need is clarity. And the idea of trying to adjust to multiple jurisdictions across the country is extremely taxing and probably a bigger tax on innovation than would be clarity across the board.

The second point I would make is that there are technologies, again, that are deployed in many other verticals that allow you to process data in privacy-compliant ways, and if these rules—if this legislation takes effect, the innovation will shift towards using those technologies. And I think that is a really good thing for consumers and a really good way for this country to lead on innovation in this space.

Mr. CARTER. Well, you know, look, all of that put together—the fact that I don't want to suppress freedom of speech, I don't want to suppress innovation, I don't want us to get behind our global competitors—that is why this is a heavy lift. We need y'all's help.

Mr. Chairman, I am out of time, and I will yield back. Thank y'all again for being here.

Mr. BILIRAKIS. Appreciate it. The gentleman yields back.

Now I will recognize, certainly last but not least—certainly not least. He has got a lot of experience in this area. So we will recognize Representative Obernolte from the great State of California. Five minutes.

Mr. OBERNOLTE. Thank you, Mr. Chair. Thank you, sir.

Ms. Rich, you said something at the end of your testimony that really resonated with me. You said that one of the primary reasons why Congress needs to act to establish data privacy standards at a Federal level is because the FTC is unable to, through rule-making, resolve the primary controversies of data privacy, those being preemption and also private right of action. I couldn't agree with you more.

So I know that Mr. Duncan asked you about preemption, and you said some level of preemption is necessary, but I wanted to tunnel down on that. Should we completely preempt away from the States this space or should we allow the States to create standards that might be more stringent than those created at the Federal level?

Ms. RICH. Well, as I have said, I think that some level of preemption is necessary for consistency. I also think we are beyond in the debate total preemption because, clearly, compromises need to be made. And I am in awe of this committee's work for making some of those hard cuts, at least attempting to.

So, you know, I think the ADPPA strikes—attempts to strike a good balance of partially preempting to create as much consistency as possible, but allowing—first of all, allowing all the State AGs and other State agencies to enforce, which is incredibly important, and then leaving certain things in place.

There is a third issue that is really controversial too that I think Congress needs to resolve, which is how much discretion the FTC should have to its own rulemaking. And so if the FTC does its rulemaking that it is doing, it has total discretion. But this body has tried to make decisions about when the FTC should be able to do rulemaking and when Congress' decisions should be the law of the land.

Mr. OBERNOLTE. Yes. Well, talking about this issue of preemption, I am going to partially agree with you. I am of the opinion we need to totally federally preempt it. And the reason that I feel that way is one of the primary justifications for preempting at all, I think, is to avoid creating this patchwork quilt of 50 different State regulations, which as has been pointed out in the testimony, very destructive to entrepreneurialism, very difficult for small businesses to deal with. And unfortunately, if we only partially preempt, we leave that problem out there, because small companies, you know, two guys in a garage in Cupertino, they are still going to have to navigate this space.

And by the way, before this I served in the California legislature. I was one of the leads in the drafting and passage of the California Consumer Privacy Act. So I am one with the vested interest of saying, "No, no, don't touch my baby." But, you know, I really firmly believe that this is something that we need to preempt. If we are going to do it, we need to do it all the way.

Mr. MUDD, we have been talking about private right of action. And let me ask you—because I know opinions have varied in the testimony here—who do you think should be responsible for enforcing whatever privacy protections we put in place? Should it be the FTC? Should it be State attorney generals? The Federal attorney generals? Should there be a private right of action? What do you think about enforcement?

Mr. MUDD. Representative, I apologize, it is not in the area of my expertise, and I would be reluctant to offer an opinion like that.

Mr. OBERNOLTE. OK. We will go back to Ms. Rich then. I know she has an opinion on this subject.

Ms. RICH. Again, I support as much consistency as possible. And so even—you know, when I was at the FTC and then at Consumer Reports, I had worries about the private right of action and some of the incentives there. I do think that between the FTC and all of the State attorneys general and all of the other agencies within the State, that is a lot of enforcers on the beat, plus the FTC really needs more resources. But we are a little bit beyond barring the entire, you know, private right of action.

Again, a lot of this is a political decision that you all need to make, and compromises have been made. And my hat is off to you guys for being able to do so.

Mr. OBERNOLTE. Sure. Well, and I think that we are all interested in getting this across the finish line. You know, the bill that we had last year, we didn't quite get it there. And so we are trying

to figure out how to tweak it to get it the rest of the way to passage, which I think is a goal we all support. I myself, though, have some very serious concerns about private right of action. And one need look no further than other domains that we have implemented it in to find out the truth of, you know, what you said in your testimony earlier, which was sometimes—in fact, quite often—it benefits attorneys more than plaintiffs.

In California, we have—I mean, obviously, we have the Americans with Disabilities Act. I am sure we are all familiar with those abuses. But in California we have had the Private Attorney General Act for the last few years that creates a private right of action for the enforcement of California labor laws. And every single one who—person who represents any piece of California can testify to the number of abusive lawsuits that have been brought, you know, clearly without the intention of actually forcing compliance with the labor law, but only through a profit motive on the part of a law firm. So that is why I think this is really difficult to navigate, and I really think that we have sufficient authority through the FTC and the State AGs to be able to enforce this.

But I see my time has expired. I want to thank you all for your testimony, and hopefully we will be able to get this across the finish line this time around.

I yield back, Mr. Chairman.

Mr. BILIRAKIS. Thank you. And the gentleman yields back.

So seeing that there are no further Members wishing to be recognized, I would like to thank all the witnesses for being here. Thank you so much for your patience. Y'all did an amazing job, you really did. I appreciate it. Very informative. So you guys don't have to stay. I have got some business to take care of. But thank you so very much.

Pursuant to the committee rules, I remind Members that they have 10 business days to submit questions for the record, and I ask the witnesses to respond to the questions promptly. If you kindly will respond, we would appreciate that. Members should submit their questions by the close of business on March 15.

So, let's see, I have got some documents that need to be entered into the record.

So, pursuant to the committee rules, I ask unanimous consent to enter the following documents into the record: a letter from the Institute of Electrical and Electronics Engineers USA; a letter from the Insights Association; a letter from the Privacy for America; a letter from TechNet; a letter from the Health Innovation Alliance; a letter from the Credit Union National Association; a letter from Engine; a letter from the Confidentiality Coalition; a letter from the National Association of Federally Ensured Credit Unions; a letter from Mr. Brandon Pugh of the R Street Institute; a letter from the National Multifamily Housing Council and the National Apartment Association; a letter from the Main Street Privacy Coalition; a letter from the Electronic Transactions Association; a letter from the BSA, the Software Alliance; a letter from the Commissioner, Peter A. Feldman, of the Consumer Protection Safety Commission; a letter from ACT, The App Association and the Connected Health Initiative; a letter from the U.S. Chamber of Commerce; a report from the Information Technology and Innovation Foundation enti-

tled “The Looming Cost of a Patchwork of State Privacy Laws”; a letter from the National Association of Manufacturers; a letter from the Leadership Conference on Civil and Human Rights; a letter from the law enforcement stakeholders; and finally, a letter from the Fraternal Order of Police and the International Association of Chiefs of Police.

Without objection, so ordered.

[The information appears at the conclusion of the hearing.¹]

Mr. BILIRAKIS. So thank you very much, folks, even in the audience, for attending this meeting. I want to thank the ranking member and, of course, the ranking member on the full committee and the chairperson, Cathy McMorris Rodgers.

And, without objection, this subcommittee is adjourned. We appreciate all of y’all. Thank you.

[Whereupon, at 12:04 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

¹The R Street Institute letter and the Information Technology and Innovation Foundation report have been retained in committee files and are available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=115376>.



28 February 2023

Representative Cathy McMorris Rodgers, Chair
House Committee on Energy and Commerce
Washington, DC 20515

Representative Frank Pallone, Jr., Ranking Member
House Committee on Energy and Commerce
Washington, DC 20515

Representative Gus Bilirakis, Chair
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
Washington, DC 20515

Representative Jan Schakowsky, Ranking Member
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
Washington, DC 20515

Dear Rep. McMorris Rodgers, Pallone, Bilirakis, and Schakowsky,

Thank you for conducting the Subcommittee's March 1st hearing on the role of standards in protecting the online privacy of Americans, in particular children. IEEE, as a leading global standards developer, believes that the standardization process is important to both promoting innovation and, as rapidly growing technologies change the way we interact and expose our personal data, ensuring that technologies do not harm users.

The U.S. has for decades consistently, and in our opinion appropriately, promoted the principles of consensus-based standards developed in a decentralized direct-participation model. These principles have contributed greatly to advancing U.S. innovations and technological competitiveness. We encourage the federal government to continue to engage actively and effectively with standards setting bodies as a means of strengthening data privacy governance.

The U.S. should lead discussions on global technical standardization and establishment of a national data privacy standard. Below are listed the IEEE standards and related programs that are most relevant to the protection of online privacy, including IEEE 2089™, a standard that establishes a framework for developing age-appropriate digital services for situations where users are children.

IEEE-USA is the American component of the global IEEE (Institute of Electrical and Electronics Engineers), the world's largest technical professional society. We represent technology professionals in all parts of our 21st century

IEEE-USA | 2001 L Street, N.W., Suite 700, Washington, D.C. 20036-4928 USA

Office: +1 202 785 0017 | Fax: +1 202 785 0835 | E-mail: ieeeusa@ieee.org | Web: <http://www.ieeeusa.org>

technology-based society – from space exploration to biotech, cryptocurrency to power generation. IEEE has more than 150,000 individual members across the United States. The IEEE Standards Association (IEEE SA) is one of the world's largest global standard setting bodies with a catalog of more than 2100 standards and projects, including many at the heart of our modern economy.

If you have any questions, please do not hesitate to contact Erica Wissolik at (202) 530-8347 or e.wissolik@ieee.org.

Sincerely,



Eduardo F. Palacio
President

IEEE Standards and Related Information

Name/Title	Description	Link
IEEE 7002™ Standard for Data Privacy Process	Defines requirements for a systems/software engineering process for privacy-oriented considerations regarding products, services, and systems utilizing employee, customer, or other external user's personal data.	https://standards.ieee.org/ieee/7002/6898/ The PDF of this standard is provided at no cost in the IEEE GET Program at https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=93
IEEE 2410™ Standard for Biometric Privacy	This standard provides for private identity assertion, and includes a formal specification for privacy and biometrics such that a conforming system will meet GDPR, CCPA, BIPA, or HIPAA privacy requirements.	https://standards.ieee.org/ieee/2410/7746/

IEEE P1912 Standard for Privacy and Security Framework for Consumer Wireless Devices	<p>This standard project (in development) defines a privacy scale for data that is defined as personal identifiable information, which is collected, retained, processed, or shared on networked edge, fog, or cloud computing devices. This privacy scale will provide input to assessment tools that developers or users of these applications employ to develop, discover, recognize, or implement appropriate privacy settings for the personal data resident on these devices.</p>	https://standards.ieee.org/ieee/1912/10174/
IEEE 2089™ Standard for Age Appropriate Digital Services Framework – Based on the 5Rights Principles for Children.	<p>This standard establishes a framework for developing age-appropriate digital services for situations where users are children. The framework centers around the following key areas: a) recognition that the user is a child, b) considers the capacity and upholds the rights of children, c) offers terms appropriate to children, d) presents information in an age-appropriate way and e) offers a level of validation for service design decisions.</p>	https://standards.ieee.org/ieee/2089/7633/
IEEE P2876™ Recommended Practice for Inclusion, Dignity and Privacy in Online Gaming.	<p>This standard project (in development) defines a set of recommended practices for inclusion, dignity, and privacy in online gaming. It includes a descriptive taxonomy to enable clear and concise communication between stakeholders, and a set of best practices designed to help game developers build more inclusive online communities. A reference model defining common concerns, challenges, and remediation methods across all online games is also included.</p>	https://standards.ieee.org/ieee/2876/10184/

IEEE 802E™ Recommended Practice for Privacy Considerations for IEEE 802® Technologies	<p>This recommended practice helps promote a consistent approach by IEEE 802 protocol developers to mitigate privacy threats identified in the specified privacy threat model, and to provide a privacy guideline.</p>	https://standards.ieee.org/ieee/802E/6242/
IEEE P2933™ Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety and Security.	<p>A set of guidelines and standards is necessary to standardize the use of clinical Internet of Things (IoT) devices for precision medicine, data sharing, interoperability, and security, with a goal of improved and measurable healthcare outcomes and protection of patient data. This standard project will establish that framework, with the incorporation of TIPPSS principles. It will encompass wearable device interoperability with healthcare systems such as electronic health records (EHR), electronic medical records (EMR), other clinical IoT devices, hospital devices, and with future devices and connected healthcare systems.</p>	https://standards.ieee.org/ieee/2933/7592/
IEEE 2883-2022™ Standard for Sanitizing Storage	<p>This standard covers methods of sanitizing logical storage and physical storage, as well as providing technology-specific requirements and guidance for the elimination of recorded data.</p>	https://standards.ieee.org/ieee/2883/10277/
IEEE 1619.1-2018™ Standard for Authenticated Encryption with Length Expansion for Storage Devices	<p>This standard specifies requirements for cryptographic units that provide encryption and authentication for data contained within storage media.</p>	https://ieeexplore.ieee.org/document/8637991

IEEE 1619.2-2021™ Standard for Wide-Block Encryption for Shared Storage Media	EME2-AES and XCB-AES wide-block encryption with associated data (EAD) modes of the NIST AES block cipher, providing usage guidelines and test vectors, are described.	https://standards.ieee.org/ieee/1619.2/10252/
IEEE 2089™ Standard for an Age Appropriate Digital Services Framework Based on the 5 Rights Principles for Children	This standard establishes a set of processes by which organizations seek to make their services age appropriate. It sets out processes through the life cycle of development, delivery and distribution that will help organizations ask the right relevant questions of their services, identify risks and opportunities by which to make their services age appropriate and take steps to mitigate risk and embed beneficial systems that support increased age appropriate engagement.	https://standards.ieee.org/ieee/2089/7633/
IEEE 2890™ Recommended Practice for Provenance of Indigenous Peoples' Data	This recommended practice details the rules by which the provenance of Indigenous Peoples' data should be described and recorded.	https://standards.ieee.org/ieee/2890/10318/
IEEE SA Industry Connection Program on Cybersecurity for Next Generation Connectivity Systems	A pre-standardization initiative addressing cyber security issues and rethinking architectures to address critical market needs. IEEE SA proposes five architecture principles or baseline realities that will be used to explore new architectures to create more secure and trusted digital platforms: passwords, phishing, data breaches, privacy erosion and surveillance, and misinformation and unverified sources.	https://standards.ieee.org/industry-connections/cyber-security-for-next-generation-connectivity-systems/
IEEE SA Industry Connections Program on Cybersecurity in Agile	A pre-standardization addressing cloud remote access security, including performing a gap analysis of existing	https://standards.ieee.org/industry-connections/cybersecurity-agile-cloud-computing/

Cloud Computing	cloud standards and certifications and evaluating the need for extending them for secured remote access. Emphasizes defense organizations which have more restricted security requirements and may require more restricted security on remote access to their data.	
------------------------	---	--



February 27, 2023

The Honorable Gus Bilirakis
Chairman

The Honorable Jan Schakowsky
Ranking Member

House Subcommittee on Innovation, Data, and Commerce

RE: March 1, 2023 subcommittee hearing on “Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy”

Dear Chair Bilirakis and Ranking Member Schakowsky,

The Insights Association (IA), the leading nonprofit trade association for the market research and data analytics industry (also known as the insights industry), is heartened by the March 1, 2023 hearing in the House Energy and Commerce Committee Innovation, Data, And Commerce Subcommittee on federal privacy legislation and your commitment to continue to try to craft a preemptive national privacy law.

IA needs to highlight three key points for the Subcommittee to consider during this hearing and as you continue work on such legislation: market research should be allowed to function; Congress should set a national privacy standard; and the Privacy for America framework provides a model approach for legislation.

1. **Market research needs to be permitted to function.** Our more than 7,100 members are the world’s leading producers of intelligence, analytics and insights measuring and defining the needs, attitudes and behaviors of consumers, organizations and their employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas. Any legislation you consider should not unnecessarily restrict companies and organizations from using data to better the products, services and ideas they offer to consumers or conduct research on the markets for their offerings (and public policies). Innovation and developments in products, services and ideas work to benefit consumers and citizens.
2. **Congress should set a national privacy standard, not the Federal Trade Commission (FTC).** The regulation of the modern economy, which is data-driven in every way, should be a matter left to the democratically-accountable legislative branch. Agencies like the FTC should act only when directly instructed to do so by Congress through specific authorities contained in legislation. A national standard for data collection and processing should be set

P R O T E C T ◆ C O N N E C T ◆ I N F O R M ◆ P R O M O T E

Insights Association | 1629 K Street NW, Suite 300 Washington, DC 20006 | Phone: 202-800-2545 | www.insightsassociation.org

at the federal level, through the clear authority granted by the American people and the Constitution in Congress.

3. **The Privacy for America Framework provides a model approach for privacy legislation.** The Subcommittee can look to the Privacy for America Principles of Privacy Legislation¹ as an example of how to strike an appropriate balance for national data standards. The Framework would designate certain uses of personal information to be reasonable and others to be per se unreasonable (and thus prohibited). The Framework prioritizes consumer protection while still preserving beneficial uses of data and access to a vibrant online ecosystem.

Thank you for your consideration of these points for your March 1st hearing. IA anticipates working closely with Congress as it continues to evaluate and develop approaches to preemptive, comprehensive, privacy legislation. Please reach out with any questions or concerns.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

CC: House Innovation, Data, And Commerce Subcommittee members

¹ Privacy for America, Principles for Privacy Legislation (2019)
<https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/>.



March 1, 2023

The Hon. Cathy McMorris Rodgers
Chair
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, D.C. 20515

The Hon. Frank Pallone
Ranking Member
House Energy & Commerce Committee
2322 Rayburn House Office Building
Washington, D.C. 20515

The Hon. Gus Bilirakis
Chairman
House Energy & Commerce
Subcommittee on Innovation, Data, and
Commerce
2306 Rayburn House Office Building
Washington, D.C. 20515

The Hon. Jan Schakowsky
Ranking Member
House Energy & Commerce
Subcommittee on Innovation, Data, and
Commerce
2408 Rayburn House Office Building
Washington, D.C. 20515

Dear Chair Rodgers, Chairman Bilirakis, Ranking Member Pallone, and Ranking Member Schakowsky:

Privacy for America is a coalition of trade organizations and companies representing a broad cross-section of the American economy. Our membership includes companies and trade associations in the advertising, travel, hospitality, media, financial services, data services, market research, and many other industries. We have long supported the creation of a comprehensive, preemptive national standard for consumer privacy. We are encouraged by the House Energy and Commerce Committee Innovation, Data, And Commerce Subcommittee's ("Subcommittee") decision to hold a hearing and continue to work on the creation of a preemptive national privacy law. We write to highlight several facts that the Subcommittee should consider during this hearing and its work going forward.

- **Responsible data-driven practices deliver over \$30,000 in value to consumers per year.** Studies found that data-driven practices used by companies supplemented consumer incomes to the tune of \$30,000 per year in free and discounted entertainment, information, and other services.¹ Congress should not create a new \$30,000 tax on consumers by disrupting the engine that drives that value.
- **Research proves that data-driven advertising is valued by consumers.** Data-driven advertising allows consumers to access near-endless free and low-cost content and services, such as research, music, news, videos, games, and more. According to a study of consumer attitudes towards data-driven advertising, more than half of consumers desire relevant ads,

¹ J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 2 (2022), <https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf>.



which are facilitated by such advertising, and a substantial majority (over 85 percent) desire personalized discounts for online products and services.²

- **Data-driven advertising creates opportunities for new, small, and growing businesses to access and thrive in the market.** Data-driven advertising fosters a competitive marketplace where small and mid-size businesses, as well as self-employed individuals, which are overwhelmingly minority-owned businesses, can compete with the economy's largest players.³ Companies of all sizes use data-driven advertising, but smaller firms and new market entrants depend on it for a significantly greater portion of their revenue.⁴
- **Congress should set a national standard, not the Federal Trade Commission.** The regulation of the modern economy, which is data-driven in every way, should be a matter left to the democratically accountable legislative branch. Agencies like the Federal Trade Commission should act only when directly instructed to do so by Congress through specific authorities contained in legislation. A national standard for data collection and processing should set once, through the clear authority granted by the American people and the Constitution in Congress.
- **Private companies should follow the law, not create their own.** When Congress speaks and sets a national framework for data practices all companies should follow that law. No company, just because of its position in the marketplace as the intermediary between consumers and publishers, should be able to interfere in the legitimate, responsible, data practices of others. This is especially true when those private actors do so to further their own financial goals to the detriment of their competitors. A federal law should prohibit such meddling.
- **The Privacy for America Framework provides model approach for privacy legislation.** The Subcommittee can look to the Privacy for America *Principles of Privacy Legislation* ("Framework") as an example of how to strike an appropriate balance for national data

² Mark Sableman, Heather Shoenberger & Esther Thorson, *Consumer Attitudes Toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates* (2013), located at https://www.thompsoncoburn.com/docs/default-source/Blog-documents/consumer-attitudes-toward-relevant-online-behavioral-advertising-crucial-evidence-in-the-data-privacy-debates.pdf?sfvrsn=86d44cea_0.

³ Nora Esposito, *Small Business Facts, Spotlight on Minority-Owned Employer Businesses*, U.S. SMALL BUSINESS ADMINISTRATION (May 2019), <https://cdn.advocacy.sba.gov/wp-content/uploads/2019/05/31131339/Small-Business-Facts-Spotlight-on-Minority-Owned-Employer-Businesses.pdf>.

⁴ Digital Advertising Alliance, *Study: Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), located [here](#); Deloitte, *Dynamic Markets: Unlocking Small Business Innovation And Growth Through The Rise Of The Personalized Economy* at 27 (May 2021), https://scontent-bos5-1.xx.fbcdn.net/v/t39.8562-6/100000000_4303078769743544_7237603050373993547_n.pdf?_nc_cat=109&ccb=1-7&_nc_sid=ad8a9d&_nc_ohc=diYsZTH66PEAX_6cORb&_nc_ht=scontent-bos5-1.xx&oh=00_AfAldldtTvWnhD6amBfDnljWEW3VTNTzhgiXULbzMJn1mg&oe=63FB1089.



standards.⁵ The Framework would designate certain uses of personal information to be reasonable and others to be *per se* unreasonable and thus prohibited.⁶ The Framework prioritizes consumer protection while also preserving beneficial uses of data and access to a vibrant online ecosystem.

* * *

Thank you for your consideration of this letter on this important topic. We look forward to working with the Congress as it continues to evaluate and develop approaches to preemptive, comprehensive, privacy legislation. Please contact us with any questions.

Sincerely,
Privacy for America

⁵ Privacy for America, *Principles for Privacy Legislation* (2019) <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/>.

⁶ Framework at Part 1, Sec. 1(Y); Sec. 3; Sec 6(G)(c).



1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

February 28, 2023

The Honorable Cathy McMorris Rodgers
Chair
House Committee on Energy and Commerce
2188 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
House Committee on Energy and Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chair McMorris Rodgers and Ranking Member Pallone:

In advance of this week's Subcommittee on Innovation, Data, and Commerce hearing titled "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy," I am writing to highlight TechNet's support for enactment of comprehensive federal privacy legislation and share TechNet's privacy policy principles as you work to advance this legislation in the 118th Congress.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents more than five million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

The need to pass a federal privacy law has never been greater. The global nature of data impacts every industry across our economy and demands a federal approach. Instead, we're seeing a growing patchwork of state privacy laws that are confusing consumers and hurting businesses, especially small businesses. Since 2018, 154 comprehensive privacy bills have been [considered](#) across 43 states, including 28 bills filed in 16 states just this year. By the end of the year, consumers and businesses in California, Colorado, Connecticut, Utah, and Virginia will all be regulated by different privacy laws. As more states pass their own



privacy laws, failure by Congress to take action will cost our economy more than [\\$1 trillion over 10 years](#), with more than \$200 billion being paid by small businesses.

This week's Subcommittee hearing is an important step to building continued momentum for the enactment of comprehensive federal privacy legislation in the 118th Congress and examining the best ways to protect consumers and promote America's global leadership in innovation. TechNet has long believed that for the data-driven economy to remain strong, we must always put the consumer first. In addition, we believe federal privacy legislation must provide harmonized, consistent, tech- and sector-neutral standards throughout the United States to provide regulatory certainty for all businesses, including new entrants, small businesses, as well as underserved and under-resourced innovators. We encourage the Committee to examine the [cost and operational impact](#) of the patchwork of state privacy laws on small- and medium-sized businesses and evaluate the rapid emergence of nuisance lawsuits impacting these same job creators in the absence of a federal data privacy law.

Your efforts to craft comprehensive federal privacy legislation during the 117th Congress demonstrated that there is bipartisan support in Congress to protect the privacy of all Americans and provide regulatory certainty for businesses. Polls overwhelmingly show that Americans across the ideological spectrum want Congress to come together to act on privacy legislation, with four in five voters in support of Congress prioritizing the passage of privacy legislation.

We stand ready to assist you in protecting American consumers, helping small businesses, and propelling our economy forward. We thank you for your commitment to advancing a federal data privacy law and look forward to working with you on this important issue. Please don't hesitate to reach out if we can be a resource on this issue or if you have any questions. I can be reached at cholshouser@technet.org or (210) 286-6276.

Sincerely,

A handwritten signature in cursive script, reading "Carl Holshouser".

Carl Holshouser
TechNet Senior Vice President



February 28, 2023

The Honorable Cathy McMorris Rodgers, Chair
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone, Ranking Member
House Energy & Commerce Committee
2322 Rayburn House Office Building
Washington, DC 20515

Dear Chairwoman McMorris Rodgers and Ranking Member Pallone,

The Health Innovation Alliance (HIA) appreciates your continued leadership on improving consumer privacy protections for people across the country. HIA is a diverse coalition of patient advocates, healthcare providers, consumer organizations, employers, technology companies, and payers who support the commonsense use of data and technology to improve health outcomes and lower costs.

As you consider modernizing our nation's privacy framework, we urge you to explicitly carve out existing healthcare laws and regulations in any legislation considered by the Committee. Health information exchange is vital to the practice of medicine and its regulation, and Congress has worked for years to facilitate the access, exchange, and use of health data for everything from preventing malpractice and improving patient care to advancing medical research.

Privacy of sensitive health information is necessary to establish trust to deliver care, enhance quality, and pay for services and products. This necessity is one reason there are so many existing laws to protect patient privacy while ensuring health data is available to those who need it.

Congress should ensure that any policies intended to rein in inappropriate use, disclosure, or sale of information do not thwart advances in medicine or stop medical research. Legislators in California had to amend the state's privacy law to avoid shutting down efforts to advance patient care and conduct clinical trials. Any federal legislation in this area should avoid this problem by carving out existing healthcare protections. The Health Innovation Alliance has already shared legislative text with the Energy and Commerce Committee to achieve this goal.

Additionally, health care is a complicated industry, and the regulation of health information is as well. As the Committee considers advancing consumer privacy protections and carving out existing regulations in health care, HIA urges consideration of the Health Data Use and Privacy Commission Act (S. 3620, 117th Congress). This legislation would establish a commission of experts to analyze whether health data privacy regulation should be updated, and if so, how. The Health Data Use and Privacy Commission Act would inform the Energy and Commerce Committee and the rest of Congress on how best to navigate healthcare regulation and modernize privacy for patients and consumers.

HIA stands ready to further assist the Committee in its important work to better protect consumer and health data. Thank you for your consideration.

Sincerely,

Brett Meeks
Executive Director



Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

99 M Street SE
Suite 300
Washington, DC 20003-3799

March 1, 2023

The Honorable Gus Bilirakis
Chairman
Energy and Commerce Subcommittee
on Innovation, Data and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Energy and Commerce Subcommittee
on Innovation, Data and Commerce
United States House of Representatives
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

On behalf of America's credit unions, I am writing about your hearing "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy." CUNA represents America's credit unions and their more than 130 million members.

Credit unions strongly support the enactment of a national data security and data privacy law that includes robust security standards that apply to all who collect or hold personal data and is preemptive of state laws. We firmly believe that there can be no data privacy until there is strong data security. Securing and protecting consumer data is important not only for their individual financial health but as a further safeguard against rogue international agents and interference by foreign governments.

Data privacy and data security are major concerns for Americans given the frequency of reports of misuse of personally identifiable information (PII) data by businesses and breaches by criminal actors, some of which are state sponsored. Since 2005, there have been more than 10,000 data breaches, exposing nearly 12 billion consumer records. These breaches have cost credit unions, banks, and the consumers they serve hundreds of millions of dollars, and they have compromised the consumers' privacy, jeopardizing their financial security.

Stringent information security and privacy practices have long been part of the financial services industries' business practices and are necessary as financial institutions are entrusted with consumers' personal information. This responsibility is reflected in the strong information security and privacy laws that govern data practices for the financial services industry as set forth in the Gramm Leach Bliley Act ("GLBA"). GLBA's protection requirements are strengthened by federal and state regulators' examinations for compliance with the GLBA's requirements and robust enforcement for violations. Several of these significant regulatory requirements and internal safeguards include:

- **Federal Requirements to Protect Information:** Title V of the GLBA and its implementing rules and regulations require credit unions to protect the security, integrity, and confidentiality of consumer information.
- **Federal Requirements to Notify Consumers:** Credit unions are required to notify their members whenever there is a data breach where the misuse of member information has occurred or where it is reasonably likely that misuse will occur.

cuna.org

- Strong Federal Oversight and Examination: Under their broad-based statutory supervisory and examination authority, the National Credit Union Administration (NCUA) and the Consumer Financial Protection Bureau (CFPB) regularly examine credit unions for compliance with data protection, privacy, and notice requirements.
- Strong Federal Sanction Authority: Under numerous provisions of federal law, credit unions are subject to substantial sanctions and monetary penalties for failure to comply with statutory and regulatory requirements.

While this extensive legal and regulatory examination and enforcement framework ensures that credit unions robustly protect consumers' personal financial information, this safety net only extends to financial institutions. As consumers' personal information is disseminated to third parties, those protections end and credit unions and their members are adversely impacted by the lax data security standards at other businesses. These loopholes must end and a comprehensive data security and privacy framework that covers all entities that collect consumer information and is preemptive of state laws must be established and this standard must hold those who jeopardize that data accountable through enforcement.

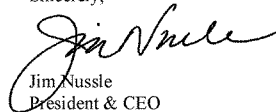
With that in mind, we ask the committee to consider the following data security and privacy principles for any comprehensive framework:

- (1) **New Privacy and Data Security Laws Should Keep GLBA Intact:** Congress should leave financial services' robust data and privacy requirements in place. Financial services and the healthcare industry are subject to federal data privacy laws. The GLBA and the Health Insurance Portability and Accountability Act (HIPAA) have protected American's PII for over two decades and should be left in place as financial services and healthcare and their respective regulators have developed regulations, guidance, and procedures for compliance.
- (2) **Data Privacy and Data Security Are Hand in Glove:** Any new privacy law should include both data privacy and data security standards. Simply put, data cannot be kept private unless it is also secured. Congress should enact robust data security standards to accompany and support data privacy standards.
- (3) **Every Business Not Already Subject to Federal Law Should Follow the Same Rules:** The new law should cover all businesses, institutions, and organizations. Consumers will lose if Congress focuses only on tech companies, credit-rating agencies, and other narrow sectors of the economy because any company that collects, uses, or shares personal data or information can misuse the data or lose the data through breach.
- (4) **There Should Be One Rule for the Road:** Any new law should preempt state requirements to simplify compliance and create equal expectation and protection for all consumers. We understand that some states have strong security and privacy requirements. Congress should carefully examine those requirements and take the best approaches from state law, as appropriate. A patchwork of state laws with a federal standard as a floor will only perpetuate a security system littered with weak links. The federal law should be the ceiling and the ceiling should be high. Just like moving away from the sector specific approach, the goal should be to create a strong national standard for all to follow.
- (5) **Breach Disclosure and Consumer Notification Are Important, But These Requirements Alone Won't Enhance Security or Privacy:** Breach notification or disclosure requirements are important, but they are akin to sounding the alarm after the fire has burned down the building. By the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions, of individuals.

- (6) **Hold Entities that Jeopardize Consumer Privacy and Security Accountable Through Regulatory Enforcement:** The law should provide mechanisms to address the harms that result from privacy violations and security violations, including data breach. Increasingly, courts are recognizing rights of action for individuals and companies (including credit unions). However, individuals and companies should be afforded a private right of action to hold those that violate the law accountable, and regulators should have the ability to act against entities that violate the law.
- (7) **Recognize This Issue For What It Is – A National Security Issue:** More and more, data breaches that expose consumer PII are perpetrated by foreign governments and other rogue international entities. The proceeds from these attacks are being used to fund illicit activity. The nature of these breaches alone calls for a strong federal response that ensures all involved in collecting, holding, and using PII do so with the security of the information of paramount concern. You simply cannot have data privacy unless there is data security.

On behalf of America's credit unions and their more than 130 million members, thank you for your consideration of our views and for holding this important hearing.

Sincerely,



Jim Nussle
President & CEO



February 28, 2023

Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Honorable Members of the Subcommittee on Innovation, Data, and Commerce:

Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Engine works with government and a community of thousands of high-technology, growth-oriented startups across the nation to support the development of technology entrepreneurship. Data-driven innovation plays a central role in technology development and entrepreneurship, and Engine accordingly appreciates the subcommittee's longstanding interest in and work toward a federal privacy framework, including by holding tomorrow's hearing on "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy."

The attached document contains high-level takeaways from forthcoming research about the impacts of the current data privacy landscape upon startups. The research is to be published in full in the coming weeks, but we wanted to share with the subcommittee because it speaks to several of the questions highlighted in the "Issues" section of the hearing memo. We hope the subcommittee finds this information useful and takes into account the experiences of startups as it explores a national standard for data privacy. Engine is committed to being a resource for the subcommittee on these and other issues impacting technology entrepreneurship.

Sincerely,

Engine
700 Penn Ave SE
Washington D.C. 20003

Startups need a federal privacy framework that works for them

Startups need a federal privacy framework that creates uniformity, promotes clarity, limits bad-faith litigation, accounts for the resources of startups, and recognizes the interconnectedness of the startup ecosystem.



Startups care about the privacy of their users and invest heavily in data privacy and security.

\$100,000 – \$300,000+

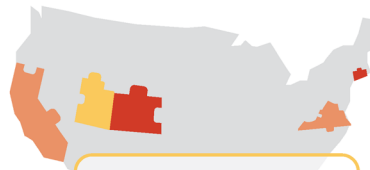
Amount individual startups have invested in their data privacy infrastructure and compliance with current or soon effective privacy laws

"We care a great deal about privacy and we want to be compliant, but it can be very expensive and complex."

Ben Brooks, Founder & CEO, PILOT, New York, NY

"Working with children, our priority is protecting their data."

Katherine Grill, Co-Founder & CEO, Neolth, Walnut Creek, CA



\$15,000 – \$60,000+

Costs individual startups spend per each additional state added to the patchwork

A patchwork of privacy laws creates confusion and duplicative costs for startups.

Five states have passed and enacted comprehensive data privacy legislation and already this year more than a dozen states have introduced at least three dozen privacy laws. The rapidly shifting landscape of state privacy laws makes compliance difficult for startups leads them to spend considerable time and resources navigating these disparate, complex frameworks.

"The rules can vary significantly on a state-by-state level. On top of that, our attorneys keep telling us that they're still changing fast, which means it's hard to have a stable, up-to-date privacy policy you feel confident is fully compliant."

Camila Lopez, Co-Founder, People Clerk, Miami, FL

"In the U.S., many states have their own rules—or no rules—and we have to approach compliance in every state on a case-by-case basis...trying to figure out how to build a business in an environment with differing rules about the same issue becomes hard and expensive."

Aditya Vishwanath, Co-Founder & CEO, Inspirit VR, Palo Alto, CA

\$55,000

Average monthly resources of a venture-backed, seed-stage startup

"As a high-growth and early-stage startup trying to grow fast, you're at a major competitive disadvantage...I would have to raise an entire second Series A to navigate many of these frameworks."

Sam Cucci, Founder & CEO IHuddle, Newark, NJ

Startups need Congress to act.

"It would be helpful to have a nationwide standard when it comes to data privacy policy, especially since we're looking to expand into new states"

Andrew Prystai, CEO & Co-Founder, EventVesta, Omaha, NE

"One uniform, consistently enforced federal policy framework could help make running RAVN easier."

Tani Chambers, Co-Founder & CEO, RAVN, New York, NY





February 28, 2023

The Honorable Gus Bilirakis
Chair
House Committee on Energy & Commerce
Subcommittee on Consumer Protection
& Commerce
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
House Committee on Energy & Commerce
Subcommittee on Consumer Protection
& Commerce
Washington, D.C. 20515

RE: March 1 “Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy” Hearing

Dear Chair Bilirakis and Ranking Member Schakowsky:

The Confidentiality Coalition thanks you for holding a hearing on, “Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy.”

The [Confidentiality Coalition](#) is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective patient privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

Accessing and appropriately sharing health data allows healthcare providers to deliver quality care and enables patients to become more engaged in their health decisions. While the Health Insurance Portability and Accountability Act (HIPAA) safeguards a specific subset of “protected health information” (PHI) and applies only to specific healthcare entities and their business associates, a vast amount of health-related information does not fall within the HIPAA regulatory framework and is largely unprotected from misuse. Today, a significant amount of personal health information is collected outside the HIPAA regulatory structure. This information should be afforded privacy and security protections that align with HIPAA. Creating protections for this information will build public trust in data collection and sharing so that the information can be used to improve health outcomes and improve the patient healthcare experience.

The Confidentiality Coalition thanks the Committee for its work on the bipartisan, bicameral "American Data Privacy and Protection Act." This bill provides a meaningful step to ensure that patients and healthcare consumers receive robust privacy protections for all their personal health information, and we look forward to working with the Committee on the safeguarding of this sensitive data. As the Committee continues its work on this important legislation, we are pleased to share the Confidentiality Coalition's "[Beyond HIPAA](#)" principles, which focus on health information not protected by the HIPAA privacy rule. These principles emphasize harmonization with HIPAA's privacy and security rules. They also advocate for individual authorization processes (including revocation of authorization) for use and disclosure of identifiable health information not covered by HIPAA. Furthermore, Coalition members support limits on the use of identifiable data beyond the expressed purpose for which authorization was given. Developing legislative and regulatory solutions to protect consumers' health information not covered by the HIPAA rules will build trust in data collection, give stakeholders better certainty about how to protect such information, and ultimately help improve health outcomes.

The Confidentiality Coalition looks forward to working with you on steps to improve privacy protections for non-HIPAA health data. Please contact me at tgrande@hlc.org or 202-306-3538 with any questions.

Sincerely,

A handwritten signature in black ink, reading "Tina O. Grande". The signature is fluid and cursive, with the first name "Tina" being the most prominent part.

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council



3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

February 28, 2023

The Honorable Gus M. Bilirakis
Chairman
Committee on Energy and Commerce
Subcommittee on Innovation, Data,
and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Janice D. Schakowsky
Ranking Member
Committee on Energy and Commerce
Subcommittee on Innovation, Data,
and Commerce
U.S. House of Representatives
Washington, DC 20515

Re: Tomorrow's Hearing, "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy"

Dear Chairman Bilirakis and Ranking Member Schakowsky:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) ahead of Wednesday's hearing, "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 135 million consumers with personal and small business financial service products. NAFCU and our members welcome the Subcommittee's review of this important issue.

As NAFCU has previously communicated to Congress, we believe there is an urgent need for comprehensive federal data privacy legislation that protects consumer data, establishes data safeguards, and recognizes the standards that have been in place for over two decades with the Gramm-Leach-Bliley Act (GLBA). In 2019, recognizing the importance of data privacy and the ongoing privacy debate, NAFCU issued a series of data privacy principles that calls for a comprehensive federal cybersecurity standard, the harmonization of existing federal data privacy laws, and the preemption of state privacy laws. As the Subcommittee works to develop much-needed comprehensive federal data privacy legislation, NAFCU recommends you include the following elements as key aspects in any such proposal:

- **A comprehensive federal cybersecurity standard covering all entities that collect and store consumer information.** Uniformly strong cybersecurity is necessary to ensure Americans' data is adequately protected across the economy. Existing strong federal cybersecurity standards, like that contained in the GLBA, should be extended to the activities of all data collectors and processors exceeding certain reasonable thresholds.
- **Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.** The current patchwork of federal and state data privacy laws generates incredible consumer confusion and significant compliance burdens while failing to address the most significant data privacy risks to Americans—those risks posed by unregulated or inconsistently regulated entities that collect, control, and process vast amounts of our data. Comprehensive federal data

The Honorable Gus M. Bilirakis
 The Honorable Janice D. Schakowsky
 February 28, 2023
 Page 2 of 3

privacy legislation should responsibly build on the successes of robust, time-tested federal laws by extending the same high data privacy standards across the economy and ensuring that already well-regulated entities, like credit unions, may confidently operate within their existing federal frameworks without fear of being subject to more than 50 different data privacy and security standards.

- **Delegation of enforcement authority to the appropriate sectoral regulator.** The National Credit Union Administration (NCUA) should be federal credit unions' sole data privacy and cybersecurity regulator. Allowing the NCUA, which is well-versed in the unique nature of federal credit unions and their operations, to continue to examine and enforce any privacy and cybersecurity requirements is the most efficient option for both credit unions and American taxpayers. Exposing credit unions and other already well-regulated entities to suits by states' attorneys general and private rights of action will dramatically increase compliance costs without providing a corresponding increase in consumer protection.
- **A safe harbor for businesses that take reasonable measures to comply with the privacy standards.** Comprehensive federal data privacy legislation should adopt principles-based requirements based on an organization's specific operations and risk profile and include a safe harbor for organizations that design and implement appropriate measures.
- **Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.** Providing multiple data privacy disclosures and opt-out mechanisms across multiple channels creates consumer confusion and unreasonable burdens for subject entities. A new privacy law should avoid conflicting or duplicative disclosure requirements by incorporating easy to understand language, like that consistent with the GLBA's disclosure requirements.
- **Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.** Actual damages to consumers are too difficult to establish by evidence, and statutory damages for violations are incredibly ripe for frivolous lawsuits. Sectoral regulators alone should have the power to assess scalable civil penalties, which can then be used to remedy and prevent consumer harm in a meaningful way.

While NAFCU supports a national data security and privacy standard, we had some concerns about the American Data Protection and Privacy Act (ADPPA) that the Committee considered in the last Congress, including:

- ***GLBA Exemption.*** Through the GLBA, Congress defined robust federal data privacy and information security standards for the financial services industries and provided the NCUA and other federal financial regulators the means with which to create and maintain strong privacy and data safeguards. The ADPPA did not recognize the long-standing requirements by providing a GLBA exemption. Congress should recognize the strength and successes of the GLBA and other time-tested federal sectoral data privacy regulation, and the value of regulator-led regulation, by wholly exempting credit unions and other already closely-regulated entities.

The Honorable Gus M. Bilirakis
 The Honorable Janice D. Schakowsky
 February 28, 2023
 Page 3 of 3

- *Private Right of Action.* This legislation provided a private right of action that would allow individuals or states' attorneys generals to sue covered entities over potential violations, allowing courts to determine the law. This means that different judicial interpretations will allow a consumer in California to have different privacy protections than a consumer in South Carolina, and credit unions will find themselves immediately and unnecessarily exposed to new and substantial compliance and legal risks.
- *Preemption of State Laws.* The ADDPA would preempt many state laws but then subsequently provided exceptions that undermine the preemption. This would perpetuate a patchwork of state and federal data privacy legislation and regulation. We believe Congress must leverage comprehensive federal data privacy legislation to expressly preempt all state data privacy legislation and regulation.

As your colleagues on the House Financial Services Committee tackle the Financial Data Privacy Act of 2023 within its jurisdiction to improve the GLBA for financial services entities, we urge the Subcommittee to craft a workable GLBA expansion to cover those outside of financial services that may be handling consumer financial data. The GLBA has successfully served consumers, credit unions, and other covered financial institutions for nearly a quarter-century. Changes to the GLBA for those already covered by it must be viewed with a cautionary eye. While some modernization of the GLBA for financial institutions may be in store, the system has generally been a success and should be a model for other areas. Making the system work best means expanding financial data protection requirements outside of just financial services. Retailers, merchants, and others that handle financial data should be subject to new requirements similar to those standards adopted for financial institutions. We urge the Subcommittee to work with your counterparts on the House Financial Services Committee to ensure a balance that recognizes existing law and the concerns of credit unions as Congress tackles the important issue of privacy reform.

NAFCU looks forward to continuing to work with you to address these concerns with consumer privacy. On behalf of our nation's credit unions and their more than 135 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information, please contact me or Amber Milenkevich, NAFCU's Senior Associate Director of Legislative Affairs, at 703-842-2238 or amilenkevich@nafcuh.org.

Sincerely,



Brad Thaler
 Vice President of Legislative Affairs

cc: Members of the Subcommittee on Innovation, Data, and Commerce



February 27, 2023

The Honorable Guy Bilirakis
Chairman
Subcommittee on Innovation, Data and
Commerce
U.S. House Committee on Energy and
Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data and
Commerce
U.S. House Committee on Energy and
Commerce
2107 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

On behalf of the members of the National Multifamily Housing Council (NMHC) and the National Apartment Association (NAA)¹, we applaud the bipartisan, bicameral work done to establish a long-overdue federal data privacy standard that protects consumers and American businesses, including apartment firms. As the House Energy and Commerce Subcommittee on Innovation, Data, and Commerce holds a hearing entitled “Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy” and renews the discussion on the American Data Privacy and Protection Act (ADPPA), NMHC and NAA wish to thank you for the bipartisan leadership on these critical issues.

Apartment owners and operators, and their service providers, rely heavily on highly sensitive, personal data about apartment applicants, residents and employees to run their day-to-day business. Therefore, they are actively engaged in these issues. Given the sensitivity of the information that apartment operators rely on and the ever-expanding cyber threat landscape we face, our industry has placed a high priority on strengthening defenses against vulnerabilities and protecting sensitive data and consumer privacy. In fact, apartment firms are committing tremendous resources to this cause.

As the Subcommittee on Innovation, Data and Commerce Subcommittee discusses the need for a national privacy standard and the ways in which the American Data Privacy and Protection Act (ADPPA) would better protect consumers, NMHC and NAA would like to share our perspective. Outlined below are NMHC and NAA’s priorities in this space, many of which are included as part

¹ For more than 25 years, the National Multifamily Housing Council (NMHC) and the National Apartment Association (NAA) have partnered to provide a single voice for America's apartment industry. Our combined memberships are engaged in all aspects of the apartment industry, including ownership, development, management, finance and suppliers partners/service providers. NMHC represents the principal officers of over 1,500 firms that own, develop, manage and finance apartments. As a federation of more than 145 state and local affiliates, NAA encompasses over 95,000 members, 141 affiliates, and more than 11.6 million apartment homes globally. The apartment industry today plays a critical role in housing this nation's households by providing apartment homes to 40.1 million residents, contributing \$3.4 trillion annually to the economy while supporting 17.5 million jobs.

of ADPPA. We believe that these priorities should serve as a starting point for any federal data privacy and security measure:

- **Federal Preemption:** ADPPA outlines a federal preemption for most existing state data privacy and security laws. NMHC and NAA believe a clear federal preemption is necessary to provide clarity for apartment firms. The current patchwork of state laws creates a significant compliance burden for apartment firms and leaves consumers vulnerable to myriad of mistakes and unintended consequences. This is particularly true given the constantly evolving nature of state data privacy and security laws.
- **Flexible and Scalable National Standard:** ADPPA reflects a need to take into consideration the data collected and the size of the company. NMHC and NAA believe any enforcement regime must provide for a flexible and scalable national standard for data security, privacy and breach notification that takes into account the needs and available resources of small businesses, as well as large firms and the sensitivity of the data in question.
- **The Ability to Continue to Perform Essential Business Functions:** ADPPA encourages data collection minimization and also rightfully acknowledges that entities may have an essential business need to engage with consumer data. Apartment firms must maintain the right to collect, use and retain sensitive information necessary for business operations. This is particularly important to ensure the safety and security of apartment residents and employees through prospective resident screening while also ensuring compliance with regulatory requirements such as reporting under the Fair Housing Act.
- **Reasonable Time Frame to Respond to Consumers:** ADPPA directs the Federal Trade Commission (FTC) to promulgate regulations for compliance by covered entities. Given the complexities of verifying any privacy or protection request and responding accurately, apartment firms need sufficient time to carry out any request, with the option for an extension if necessary.
- **Third-Party/Service Provider Responsibilities:** ADPPA makes an important distinction between covered entities, service providers and third parties. We believe that service providers must hold responsibility for their own security and privacy safeguards. Liability for any third-party/service provider security lapse or privacy violation must not shift to apartment firms or other primary consumer relationship holders. Often, businesses of all sizes are faced with the reality of being forced to accept boilerplate contractual language when contracting with a service provider or supplier. For example, while one large company may have the market share and financial leverage to negotiate and demand certain security protocols, the vast majority of American businesses do not. The responsibility for overseeing a third party's data security program and consumer privacy safeguards should remain with the party that is collecting, using and retaining sensitive information—not with apartment companies or other firms that rely on third party services.
- **Assignment of Financial and Legal Liability:** ADPPA establishes the need to differentiate between a covered entity, their service provider or a third-party data collector. We support a clear assignment of financial and legal liability to the entity that actually suffered the data breach or caused the consumer privacy violation, particularly in the case of third-party breaches or security incidents. NMHC and NAA encourage apartment operators to

ensure that service provider contracts include strong and specific language governing data security, incident response and breach notification. Unfortunately, this can often be a significant challenge, especially for smaller property owners. For this reason, the law should be clear on this point.

- **Clarity in FTC's Role in Rulemaking and Enforcement:** ADPPA designates enforcement will be carried out by the FTC. Should the FTC take on the role as regulator of data privacy and security laws, the scope of their rulemaking and enforcement role should be clarified to allow for entities to have a reasonable amount of time to respond to FTC and consumer inquiries. Additionally, entities that must comply with new data privacy and security regulations stemming from this legislation will need education, flexibility and the right to cure when the FTC notifies the entity of a possible violation before any enforcement action is taken.

We thank you for the opportunity to present the views of the apartment industry as you continue deliberations to enhance consumer privacy and data security standards. NMHC and NAA stand ready to work with Congress to create a federal data privacy and protection standard that recognizes the unique nature and needs of the apartment industry while ensuring the data that our members collect, use and maintain is secure.

Sincerely,



Sharon Wilson Géno
President
National Multifamily Housing Council



Robert Pinnegar
President & CEO
National Apartment Association



February 28, 2023

The Honorable Cathy McMorris Rodgers
Chairman
U.S. House Committee on Energy and
Commerce
Washington, D.C. 20515

The Honorable Gus Bilirakis
Chairman
U.S. House Subcommittee on Innovation,
Data, and Commerce
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
U.S. House Committee on Energy and
Commerce
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
U.S. House Subcommittee on Innovation,
Data, and Commerce
Washington, D.C. 20515

RE: Hearing on “Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy”

Dear Chairman Rodgers, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky:

We appreciate your hosting the hearing entitled, “Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy” on March 1. As the first subcommittee hearing held by the Energy and Commerce Committee on data privacy in the 118th Congress, the Main Street Privacy Coalition (MSPC) wishes to introduce ourselves to the new committee members as we look forward to continuing to work collaboratively with you and your staff to enact a preemptive federal data privacy law that establishes a uniform national standard for data privacy that protects all American consumers and requires all businesses handling consumers’ personal information to protect that data and honor consumers’ rights requests with respect to it.

The MSPC is comprised of 19 national trade associations that together represent more than a million American businesses—a broad array of companies that line America’s Main Streets¹. From retailers to Realtors®, hotels to home builders, grocery stores to restaurants, gas stations to travel plazas, self-storage to convenience stores, including franchise establishments, MSPC member companies interact with consumers day in and day out. Our members’ businesses 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 industries that MSPC member associations represent directly employ approximately 34 million Americans and constitute over one-fifth of the U.S. economy by contributing \$4.5 trillion (or 21.8%) to the U.S. gross domestic product (GDP). Our success depends on maintaining *trusted* relationships with our customers and clients: trust that goods and

¹ The Main Street Privacy Coalition website and member list may be accessed at: <https://mainstreetprivacy.com>.

services we provide are high quality and offered at competitive prices; and trust that information customers provide to us while we are serving them is kept secure and used responsibly. For these reasons, our associations are actively engaged in the discussions by policy makers surrounding data privacy protections in U.S. legislation and regulations.

MSPC firmly believes that consumers across the country should be empowered to control their personal data. Having data privacy and security laws that create clear protections for Americans while allowing our members' businesses to serve their customers in the ways they have come to rely upon is a key goal. Achieving that goal, however, has been elusive. One of the challenges central to this legislative effort is that the overwhelming focus on the data practices of so-called "big tech" companies in public policy debates can blind us to the fact that privacy law must also work for Main Street businesses interacting with consumers daily.

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 policymakers consider legislative and regulatory solutions to address data privacy concerns, our coalition urges adoption of federal privacy legislation that meets the following core principles:

- **Establishing Uniform Nationwide Rules and Enforcement for Data Privacy** – We should have a sensible, uniform federal framework for data privacy legislation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws by enacting a set of nationwide rules for all businesses handling consumers' personal data is necessary to achieve the important, national public policy goal of establishing uniform consumer privacy protections.
- **Industry Neutrality and Equal Protection for Consumers Across Business Sectors** – Federal data privacy frameworks should apply requirements to all industries that handle personal data and not place a disproportionate burden on certain sectors of the economy while simultaneously alleviating other sectors from providing equal protection of consumer data. An equivalent data privacy standard should apply, regardless of whether a business directly collected data from a consumer or obtained it in a business-to-business transaction.
- **Direct Legal Obligations (Rather than Contractual Requirements Alone) for All Entities that Handle Consumer Data** – Effective consumer protection law cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. Data service providers and other third parties need direct statutory obligations to ensure they comply with the relevant privacy scheme, particularly those offering transmission, storage, analytical processing or other consumer data services for thousands of businesses.

Main Street Privacy Coalition
 February 28, 2023
 Page 3

- **Preservation of Customer Rewards and Benefits** – Any federal data privacy framework should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships and set the terms of those relationships. Legislation should include safe harbors to ensure that consumers can purchase, or otherwise obtain, the goods and services they want by taking advantage of benefits, incentives, or enhanced services they earn from being loyal customers, even if other customers choose not to engage in such programs.
- **Transparency and Customer Choice** – Consumers deserve to know what categories of personal data businesses collect and how that data is generally used. These policies should be clearly disclosed in company privacy policies and readily accessible to consumers. These obligations should apply to all businesses handling consumers' personal data, including service providers, third parties, and financial services businesses.
- **Accountability for Business's Own Actions** – Privacy legislation should not include terms that could potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of a business partner. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability if other types of businesses do not fulfill their own obligations under the regulation.
- **Data Security Standards** – A federal data privacy law should include a reasonable data security standard for all businesses handling consumer data, as well as a uniform process for businesses suffering a data security breach to notify affected individuals. Currently, consumer-facing industry sectors are required to comply with 54 state and U.S. territorial laws on data breach notification requirements, and nearly half of the states have enacted data security laws. However, financial institutions and service providers are often exempt from these state breach notice requirements. All businesses handling consumers' data should be statutorily required to protect personal data and provide notice of their own security breaches when they occur.

We appreciate the Committee's work with MSPC last year to address our concerns within the American Data Privacy and Protection Act (ADPPA) such as strengthening the obligations for service providers handling controllers' customer information and preserving customer loyalty, rewards, and benefits programs. We would like to continue to work with the Committee this Congress to address MSPC's remaining concerns by strengthening the preemption language to ensure consistent rules to protect privacy across the nation and by adding protections to ensure that good actors complying with the law do not face abusive lawsuits (and threats of lawsuits).

Finally, we note that the House Committee on Financial Services today marked up H.R. 1165, the "Data Privacy Act of 2023," to update current privacy requirements for the financial sector regulated by the Gramm-Leach-Bliley Act. We shared our concerns in a [letter](#) to the Committee ahead of its markup addressing the inconsistencies between H.R. 1165 and the

Main Street Privacy Coalition
February 28, 2023
Page 4

ADPPA that create significant concerns for Main Street businesses. Ultimately, MSPC would like to work with both committees to ensure the bills reported by each are harmonized in a way that creates consistent rules across industry sectors and does not cause unwarranted liability on businesses in one sector for privacy practices that businesses in another sector control.

The guiding principle should be the American consumer herself, who expects her data to be protected by all businesses handling it in an equivalent way and that her privacy rights with respect to her data will be honored to the same extent by all of them. After all, the consumer's data is the same, and the protections should be the same regardless of who handles it.

Members of the MSPC – many of whom struggled to remain open to serve consumers during the COVID-19 pandemic and are facing historic pressures from the confluence of inflation, supply chain constraints, and labor shortages – look forward to collaborating with you to meet our shared goals of effectively protecting privacy in a uniform way that works for both consumers and Main Street businesses alike.

Sincerely,

Main Street Privacy Coalition

cc: Members of the U.S. House Committee on Energy and Commerce



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

March 1, 2023

The Honorable Gus Bilirakis
Chairman
Subcommittee on Innovation, Data,
and Commerce
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data,
and Commerce
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

On behalf of the Electronic Transactions Association (ETA), I appreciate the opportunity to submit this statement for the record before the Subcommittee's hearing, "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy."

ETA is the world's leading advocacy and trade association for the payments industry. Our members span the breadth of significant payments and fintech companies, from the largest incumbent players to the emerging disruptors in the U.S. and in more than a dozen countries around the world. ETA members make commerce possible by processing approximately \$44 trillion annually in purchases worldwide and deploying payments innovation to merchants and consumers.

ETA and its members support U.S. and international efforts to strengthen privacy laws in ways that help the industry combat fraud and help consumers understand how their data is being used. As lawmakers and regulators explore additional ways to protect consumers, it is critical that the government coordinates with the payments industry to combat fraud and cybercrime so that all consumers have access to safe, convenient, and affordable payment options and other financial services.

A robust financial system is integral to the economy because it enables the fundamental functions of economic activity, including connecting borrowers with savers, facilitating investments, processing payments, and safekeeping financial assets. For the U.S. financial system to remain competitive in the global economy, the U.S. must continue to prioritize consumer protection, safety, and reliability, while also continuing to lead in innovation.

ETA looks forward to encouraging a collaborative approach and believes a framework should include the following principles:

Permissible Use to Fight Fraud

The payment industry has a long commitment and history of fighting fraud and is constantly developing and deploying new technology to detect, deter, and eliminate fraud. New and enhanced technologies have amplified the payments industry's ability to offer new fraud solutions and strengthen our on-going efforts. Any privacy or data protection standard should include provisions for permissible uses of data to prevent fraud and protect consumers.

Creating A Uniform National Standard and Enforcement

Consistent protections provided by a uniform national law will benefit consumers and businesses. A federal uniform standard will provide certainty and consistency for businesses and consumers in lieu of having to navigate a complex patchwork of state laws and regulation. A uniform standard – that is a ceiling – would also reduce the complexity and costs of compliance and enforcement.

To protect consumer rights and provide responsibility, enforcement needs to be consistent and coordinate between the federal government and the state's regulatory agencies. Collaboration between the





1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

appropriate federal agency and state attorney generals should be followed to avoid duplicate or conflicting enforcement actions. However, a privacy law should not provide a private right of action for enforcement.

Industry and Sector Neutrality

A national privacy framework should be applied to all industry sectors that handle consumer data and such protections should be consistent for companies across products and services. It should also be technology neutral and allow organizations to adopt privacy protections that are appropriate to specific risks. Protections shouldn't interfere with innovation and economic competitiveness in an evolving technology landscape.

Keeping Pace with Innovation

ETA supports a privacy framework that applies to financial services in a manner that is consumer centered and risk-focused while encouraging innovation. To that, ETA supports policymakers setting principles-based guidelines for industry-led standards to meet. This would permit flexibility over time to accommodate the technology capabilities of various stakeholders and satisfy consumer expectations.

Access to Data

Individuals must have a reasonable right to access the personal information they have provided to a company and, where practical, the right to have that information corrected. Individuals should also have the ability to request the deletion of personally identifiable information provided to companies, unless there is a legitimate or legal obligation to retain that information.

* * *

The payments industry never rests — we are working tirelessly to fight fraud and protect consumers by developing new tools to prevent or identify fraud data analysis as well as by frequently introducing new fraud-fighting solutions. Privacy laws should continue to recognize these goals and the important role the payments industry plays in combating fraud. By working together, lawmakers, regulators, and industry participants can protect consumers while providing them with access to the safest and most convenient payments system in the world.

ETA would like to thank the Subcommittee for this opportunity to provide this statement for the record on this important topic. We appreciate your leadership on this important issue. If you have any questions, please contact me or ETA's Senior Vice President of Government Affairs, Scott Talbott, at stalbott@electran.org.

Sincerely,

Jeff Patchen
Director of Government Affairs
Electronic Transactions Association





March 1, 2023

The Honorable Gus Bilirakis
 Chairman
 Innovation, Data, and Commerce Subcommittee
 2306 Rayburn House Office Building
 Washington, DC 20515

The Honorable Jan Schakowsky
 Ranking Member
 Innovation, Data, and Commerce Subcommittee
 2408 Rayburn House Office Building
 Washington, DC 20515

RE: Hearing on a National Standard for Data Privacy

Dear Chairman Bilirakis and Ranking Member Schakowsky:

Thank you for convening today's hearing on establishing a national standard for data privacy. Every day, American consumers share their personal information with countless businesses just by using routine products and services. Consumers deserve to know that their data is being used responsibly. As more states consider or advance comprehensive privacy legislation, consumers and businesses alike face the possibility of fragmented regulatory regimes that could prove to be difficult to both navigate and enforce. A strong national data privacy standard will provide consumers and businesses the certainty they deserve.

BSA | The Software Alliance is the leading advocate for the global software industry.¹ Our members are enterprise software companies that create the business-to-

¹ BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

The Honorable Gus Bilirakis
 The Honorable Jan Schakowsky
 Page three
 March 1, 2023

business technology products and services that power the digital transformation of companies in every industry. BSA members provide cloud storage services, customer relationship management software, human resource management programs, identity management services, and remote collaboration software, along with a range of other enterprise technology products.

BSA commends the Energy and Commerce Committee's efforts and progress towards advancing a strong federal privacy law in the 117th Congress through the bipartisan committee passage of H.R. 8152, The American Data Privacy and Protection Act (ADPPA). Additionally, we appreciate the Committee's engagement with a broad range of stakeholders, including industry, to ensure that any federal privacy law is both effective and workable.

This Congress has a real opportunity to enact a comprehensive federal privacy law on a bipartisan basis. Passing a strong federal privacy law is a pillar of BSA's National Agenda for Digital Transformation,² and today's hearing represents an opportunity to build upon the momentum developed last Congress. Specifically, BSA urges Congress to enact a federal privacy law that (1) establishes consumers' rights in their personal data; (2) imposes strong obligations on companies that require them to handle consumers' data responsibly; and (3) provides strong and consistent enforcement. A federal privacy standard should:

- *Establish Consumer Rights.* A federal privacy law should create new rights for consumers, including the rights to access, correct, and delete their personal data, as well as the right to opt out of the sale and sharing of their personal information. These rights can help provide consumers control over their information and increase their ability to both trust and verify how their data is used.
- *Create Clear Obligations for Businesses to Handle Data Responsibly.* A federal privacy law should place meaningful limits on businesses that handle consumers' personal data and require them to handle consumers' data responsibly. Those limits should also reflect a business's role in handling consumer data, including whether a company decides why and how to collect a consumer's personal data, or instead acts as a service provider that processes a consumer's data on behalf of another company and pursuant to that company's instructions. The distinction between these two types of companies is critical to a host of privacy laws worldwide, which recognize that both types of businesses have important responsibilities and obligations to safeguard consumers' personal data and that those obligations must reflect how the

² <https://www.bsa.org/files/policy-filings/01182023uspolicyagendaltr.pdf>

The Honorable Gus Bilirakis
The Honorable Jan Schakowsky
Page three
March 1, 2023

company interacts with consumers' data to avoid creating new privacy and security risks for consumers.³

- *Provide Strong and Consistent Enforcement.* Effective enforcement is important to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. A federal privacy law should not be enforced by a single regulator, but by federal and state agencies working together. We support enforcement of a federal privacy law not only by the FTC but also all state Attorneys General, to create consistent and effective enforcement.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome and look forward to further engagement with the Committee on these important issues.

Sincerely,



Craig Albright
Vice President, US Government Relations

CC:
The Honorable Cathy McMorris Rodgers
The Honorable Frank Pallone

³ See BSA, *Controllers and Processors: A Longstanding Distinction in Privacy*, available at <https://www.bsa.org/files/policy-filings/10122022controllerprodistinction.pdf>.



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
 4330 EAST WEST HIGHWAY
 BETHESDA, MD 20814
 COMMISSIONER PETER A. FELDMAN

March 1, 2023

The Honorable Gus Bilirakis
 Chairman
 Subcommittee on Innovation, Data,
 and Commerce
 United States House of Representatives
 Washington, DC 20510

The Honorable Jan Schakowsky
 Ranking Member
 Subcommittee on Innovation, Data,
 and Commerce
 United States House of Representatives
 Washington, DC 20510

Dear Chairman Bilirakis and Ranking Member Schakowsky:

I write to thank you for holding today's hearing on "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy," and to thank you for your efforts to craft a strong national data privacy law that will advance consumer interests and interstate commerce.

As the House Energy and Commerce Committee develops legislation in this area, I hope it will also consider the impact of certain privacy provisions on the ability of retailers, manufacturers, and others to conduct efficient recalls of hazardous consumer products. I am concerned with "Right to Delete"-style provisions, for example, the one contained in the the California Consumer Privacy Act (CCPA), which limit the ability of firms to collect and use consumer data for direct notice recalls.¹

The U.S. Consumer Product Safety Commission (CPSC) is an independent federal regulatory agency responsible for protecting the public from unreasonable risks of injury and death associated with consumer products. Because CPSC is not a privacy regulator, I take no official position on the merits of broader consumer privacy considerations. However, given CPSC's extensive work on consumer product recalls, I would like to call your attention to the ways in which CPSC and recalling firms rely on industry-collected personally identifiable information (PII) of customers purchasing consumer products to advance safety.

CPSC is currently exploring innovative ways to effect consumer notification.² These efforts would be severely limited without access to the consumer data such "Right to Delete" provisions seek to restrict.

¹ California Consumer Privacy Act of 2018, ch. 55, 2018 Cal. Stat. 91 (codified at Cal. Civ. Code tit. 1.81.5); Cal. Civ. Code § 1798.105 (effective Jan. 1, 2020); Cal. Civ. Code § 1798.120 (effective Jan. 1, 2020).

² Sean Oberle, *Innovative Consumer Notification is a CPSC Theme at ICPHSO*, 52 PROD. SAFETY LTR., Feb. 27, 2023, <https://productsafetyletter.com/Content/8802.aspx>.

Hon. Bilirakis and Hon. Schakowsky

March 1, 2023

Page 2

To improve recall effectiveness, CPSC compliance staff works with manufacturers, distributors, and retailers to develop mutually acceptable programs that include a variety of notification methods to alert affected consumers about product recalls. Research shows, and the CPSC has long recognized, a powerful positive relationship between direct notification of consumers and recall success.³ Direct notification is not possible without affected consumers' PII. Often, CPSC will encourage a recalling firm to use the information it collects through registration cards, sales records, catalog orders, retailer loyalty cards, or other means, to effect direct notification.⁴ In other situations, companies may purchase commercially-available mailing lists of consumers who are likely to use a particular product.⁵ Industry-collected consumer PII, and the direct notification it enables, is an important tool to locate and remove hazardous product as quickly as possible.

Because existing state "Right to Delete" provisions could result in the deletion of this critical consumer PII, it is my hope that you will consider the importance of preserving the ability of firms to conduct efficient transmission of recall notifications. To that end, the Committee should consider language that provides a national and uniform federal framework that recognizes product recalls as a legitimate use of consumer PII. Also, federal privacy legislation should include an exemption for consumer safety and recall efficiency.

Thank you for your attention to this matter. As always, I am available to assist you in any way I can.

Sincerely,

Peter A. Feldman
Commissioner

cc: The Honorable Cathy McMorris Rodgers Chair Committee on Energy and Commerce U.S. House of Representatives	The Honorable Frank Pallone Ranking Member Committee on Energy and Commerce U.S. House of Representatives
--	--

³ See e.g., Dennis R. Murphy & Paul H. Rubin, *Determinants of Recall Success Rates*, 11 J. OF PROD. LIAB. 17, 17-28 (1988); and see U.S. CONSUMER PROD. SAFETY COMM'N, RECALL EFFECTIVENESS WORKSHOP REPORT 5 (2018), available at https://www.cpsc.gov/s3fs-public/Recall_Effectiveness_Workshop_Report-2018.pdf?R1VYLtU18M_id.2vkAKIH0UZjaSCab (last visited Mar. 1, 2023) (CPSC staff finding that "[d]irect notice recalls have proven to be the most effective recalls").

⁴ See U.S. CONSUMER PROD. SAFETY COMM'N, RECALL HANDBOOK 19 (2012), <https://www.cpsc.gov/s3fs-public/8002.pdf> (last visited Mar. 1, 2023).

⁵ Because such lists are generally available from business that sell personal information about consumers to third parties, the CCPA "Right to Opt-Out" provision raises additional concerns with respect to the commercial availability, accuracy, and completeness of consumer PII for these purposes. See Cal. Civ. Code § 1798.120 (effective Jan. 1, 2020).



Hearing: Promoting U.S. Innovation And Individual Liberty Through A National Standard For Data Privacy

House Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce
Statement for the Record of Morgan Reed

President, ACT | The App Association and Connected Health Initiative

Dear Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee:

Thank you for the opportunity to provide input for this hearing on data privacy, one of the most important pillars of the internet age. ACT | The App Association's (the App Association's) Connected Health Initiative (CHI), is a multistakeholder coalition with a shared interest in ensuring the public policy landscape enables and encourages the use of digital health tools that improve outcomes and help control the costs of care. CHI's interest in federal privacy law under the Subcommittee on Innovation, Data and Commerce's (IDC's) jurisdiction has grown in concert with the expansion of digital health information that is created or transferred outside the scope of the Health Insurance Portability and Accountability Act (HIPAA). In the latter days of a global pandemic that forced virtual care adoption and in the middle of a crushing physician shortage set to increase to up to 122,000 by 2032,¹ digital health tools like remote monitoring and telehealth platforms are playing a more important role than ever. Patients, providers, and consumers must be able to trust that innovators in this space are protecting the security and privacy of sensitive personal information.

Introduction

The App Association has long called for a strong national data privacy law, and CHI has also put forth principles for a federal privacy law of general applicability. The biggest problem with the privacy landscape is the mismatch between consumers' expectations of their privacy and the reality of how many entities buy, sell, and use their data. We have all experienced the phenomenon of discussing a topic with friends and getting served a targeted ad shortly after. While we feel as though our phones are spying on us, companies are actually using our online behavioral data to predict other things in which we might be interested. We willingly consent to the collection and use of our data in this way through the terms and conditions of signing up for nearly any online account—for rideshare apps, social media sites, online retail, and web-enabled consumer health products, to name just a few. And we rarely think about the implications of these conditions afterward.

¹ Assoc. of American Medical Colleges, "New Findings Confirm Predictions on Physician Shortage," press release (Apr. 23, 2019), available at <https://www.aamc.org/news-insights/press-releases/new-findings-confirm-predictions-physician-shortage>.

A comprehensive national privacy policy would help consumers understand where their data is located, who has access to it, and what their rights are surrounding the sale or use of it. Especially in the health care space, consumers need to be protected from actors looking to misuse their data and expose them to risk. Many consumers misunderstand the protections afforded to them by existing laws like HIPAA or Federal Trade Commission (FTC) regulations. Instead of modifying or expanding these existing laws and regulations, Congress should create a new, privacy-focused law that covers all kinds of consumer data.

Consumers and Companies Alike Usually Misunderstand HIPAA

At its core, HIPAA focuses on the portability and interoperability of health data. Congress designed it to ensure that consumers can change insurance providers or primary care physicians without having their data hoarded by those entities. The original text of the law did not include a privacy requirement, but instead required the Department of Health and Human Services (HHS) to promulgate a rule on privacy standards three years after enactment if Congress failed to pass a national set of privacy requirements for entities regulated under HIPAA.² Since HHS promulgated the Privacy Rule under the existing, limited authorities granted to it under the original HIPAA statute, it could break no new ground on protecting privacy and only worked within its interoperability-driven mandate. This legislative and regulatory history helps explain why the HIPAA Privacy Rule exhibits otherwise surprising levels of permissiveness and interoperability rather than protection and patient control of personal health data. And now, the explosion of health data held by a wide variety of entities not covered under HIPAA means that much of our health data is not covered by a Privacy Rule that is not a good fit for it in the first place.

Most consumers do not understand this misalignment. A 2019 Pew Research study found that 63 percent of Americans say they understand very little or nothing at all about the laws and regulations that are currently in place to protect their data privacy.³ To complicate the picture further, there are many cases that consumers might think are covered but are not because of the construction of the HIPAA Privacy Rule. For example, HIPAA rules mostly do not apply to vendors of public health records (like fitness trackers), payment processors (like banks), and even some doctors who do not bill through electronic claims to insurance plans.⁴ These are all instances where Americans without an understanding of the limitations of the HIPAA privacy rule could reasonably expect their data to be protected, but it is not.

² *Health Insurance Portability and Accountability Act of 1996* (P.L. 104-91).

³ <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>

⁴ HIPAA Privacy Rule, 45 CFR 160 and 45 CFR 164 subparts A and E.

HIPAA regulations are difficult for companies to understand as well. The definitions of “covered entity” and “business associate” have many nuances, and it is often hard for small businesses like App Association members to determine whether they are subject to the regulations. To help our members and other similar organizations, the App Association created a resource to check for whether they are a covered entity or a business associate. If a business focused on healthcare data has difficulty in understanding its legal obligations, it is not reasonable to expect consumers to understand their rights and protections under the law.

Any national privacy legislation Congress passes must avoid overly burdensome, duplicative, and even unsafe requirements for those entities already required to comply with HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The patient-provider relationship makes some of the general privacy provisions in the major bills under consideration inappropriate for HIPAA covered entities and business associates. For example, deletion of data may pose a safety hazard to patients and staff in the context of clinical care. Thus, Congress should keep HIPAA and HITECH in place and carve a general federal privacy law around them. However, we recommend that such a law adopt an approach to sensitive data, including health data, that is roughly consistent with HIPAA’s requirements.

Notwithstanding its shortcomings as a federal privacy law of general applicability, HIPAA requires robust protections for patients tailored to healthcare that should be maintained. Patients have come to rely on a federal healthcare regime that generally keeps their health records out of circulation. However, despite its interoperability roots, HIPAA’s de-emphasis on patient control over health records helped contribute to a situation where, perversely, patients have struggled to bring their records with them to new providers efficiently. But more relevantly here, it also rendered patients essentially unable to port their health information outside the HIPAA umbrella. Responding to this unintended consequence, Congress enacted the 21st Century Cures Act, which required the sub-agency that enforces HIPAA, the Office of Civil Rights (OCR), to prohibit “information blocking” by HIPAA covered entities and business associates. Although OCR is not yet enforcing the information blocking rule, it is already applying additional pressure on Congress to establish a privacy framework to address risks to health information once a patient requests its transfer to non-HIPAA entities as the information blocking rules contemplate. To help orient patients, providers, and consumers to those risks—and to bolster FTC enforcement in these scenarios—CHI suggested that the information blocking rules require any non-HIPAA covered entities receiving health information on behalf of patients make a few high-level attestations as to their privacy and data security practices. This approach is no substitute for a federal privacy law. However, it would help address the perceived and actual privacy and security disparities between the HIPAA environment and the rest of the American economy. For the information blocking rules to work as intended, Congress should enact a federal privacy framework.

Some advocates have proposed that, instead of working out compromise general privacy protections, Congress should expand HIPAA to cover health-related data collection and processing activities across the rest of the economy. However, as alluded to above, policymakers would need to rework HIPAA extensively to support such an expansion. Rules around covered entities, business associate agreements, types of data covered, and reasons for triggering coverage would all need to be radically altered. In addition, the HIPAA Privacy Rule is not law but an agency rule and could be changed if the agency chooses. HHS also does not have the budget, personnel, or authority to oversee a large expansion of the scope of the HIPAA Privacy Rule. Because of the permissiveness of the original law, the limited circumstances covered by it, and the difficulty in understanding requirements, expanding HIPAA—and OCR—to police the entire economy is not likely to be the best approach. We need a comprehensive privacy law that would protect all kinds of data, including sensitive health information. Similarly, a federal law of general applicability should avoid accidentally imposing its requirements on Protected Health information (PHI) subject to HIPAA, which would result in unintended consequences explored in more detail below.

Data use disclosures do not work for consumers

While not federally required (except in the case of users under 13 years of age), many websites and apps have privacy policies and terms and conditions of data collection and use. They notify consumers of those policies primarily through long documents, sometimes hiding the fact that many companies generate significant revenue through the sale and collection of data. Sometimes, apps or websites will push a shorter notification to a user's device to inform them of the applicability of a certain part of the policy. While none of the available methods is a perfect way of conveying dense information quickly, the in-time notices tend to be more effective since they appear more seamlessly in the context of the consumer's engagement with an online service. However, there is no easy way to increase the usefulness of such notices without a clear and universal privacy law that would outline the basic requirements of such disclosures. To operate in an increasingly online world, consumers should understand how their data is being collected, what it is being used for, and who has access to it. A national privacy law would take steps toward ensuring this future.

We need strong federal privacy protections

This Committee has made significant progress in negotiations toward a compromise federal privacy bill over the past few years. The remaining disagreements are understandable, but I urge you to find a middle ground on these issues in order to establish long-overdue protections for patients and consumers for the processing and collection of their health data. Although the FTC takes an active role in enforcing the prohibition on unfair or deceptive acts or practices (UDAP), other agencies also have jurisdiction, such as the Department of Health and Human Services (HHS), to enforce

industry-specific privacy and security requirements. Left to its own devices and with incomplete authorities from Congress, the FTC is working with limited resources, such as interpreting its data breach notification requirements to cover privacy harms.⁵ Although this may have some of the deterrent effects the FTC intended, it is ultimately a confusing interpretation of rules Congress drafted to apply in instances of unauthorized access to data—as opposed to situations where health apps share data purposefully with third parties.⁶ A more fundamental question is how government should regulate the aggregation and monetization of sensitive health information outside HIPAA's scope and the FTC's limited ability to directly address the associated risks.

Consumers, patients, and innovators in connected health deserve a more certain and comprehensive legal framework for regulations applied to digital health companies to guide their collection and processing activities involving sensitive information like health data. Similarly, explicit privacy prohibitions would better equip the FTC to prevent likely privacy harms involving health data, instead of waiting until harmful conduct has occurred and then seeking to prohibit the activity under its UDAP authority. As you work toward a compromise, we encourage you to keep the following guiding principles in mind with respect to healthcare privacy:

1. **Individual Rights.** Where practicable, legislation should require covered companies to provide individuals access to their data, the ability to amend incorrect information, and to direct entities to not sell their health data that those companies collect or maintain. In some situations, a right to data deletion may be allowed, unless patient safety or other risks are likely. Accordingly, we agree with the drafters of the major privacy bills under consideration in Congress that the obligation to honor data deletion requests should not extend to HIPAA covered entities or business associates, underscoring the need for legislation to carefully exclude data subject to HIPAA and associated privacy requirements. Privacy rights should be honored unless they are waived by an individual in a meaningful way.
2. **Transparency and Consent.** Where appropriate, legislation governing electronic data in apps should require covered companies to obtain affirmative, opt-in consent for sensitive information, including health data, informed by clear disclosures as to how covered companies collect, use, store, protect, and share health data, and for what purpose a covered company collects or processes such data. Terms should be clearly defined and unambiguous, and this should be more than a “check the box” process to use an app.

⁵ Fed. Trade Comm'n, Statement of the Commission on Breaches by Health Apps and Other Connected Devices, (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/rules/health-breach-notificationrule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

⁶ See letter from Morgan Reed, president, ACT | The App Association, to United States House of Representatives Committee on Energy and Commerce, Re: *Flo Health, Inc.*, Fed. Trade Comm'n complaint (Feb. 17, 2021).

3. **Civil Rights.** Legislation should clarify the FTC's role in assisting other federal agencies tasked with enforcing discrimination laws, where appropriate, against entities that process health data in a manner that results in harmful bias or discrimination. The FTC should, in collaboration with those federal agencies, protect individuals' civil rights and work to evaluate the potential risks posed by algorithms, particularly as inferences are drawn from individuals' sensitive health data.
4. **Data Security.** Legislation should require covered companies to maintain a comprehensive security program that is designed to protect the security, privacy, confidentiality, and integrity of health data against risks—such as unauthorized access or use, or unintended or inappropriate disclosure—through the use of reasonable administrative, technological, risk management, and physical safeguards built into the design of their applications, products, or services to appropriately protect the data. These programs should be scalable and technology neutral.
5. **Data Minimization and Access Restrictions.** Legislation should require companies to limit health data processing, transfer, and collection to those activities that are reasonably necessary, proportionate, and limited to provide a product or service specifically requested by an individual, reasonably anticipated within the context of a company's ongoing relationship with an individual, or meeting a particular purpose identified publicly on a company's website or marketing materials. Legislation should also require companies to limit internal access to health data to only those employees or third-party service providers whose access is necessary to provide or improve products or services to the individual to whom the data pertains, within the context of the company's ongoing relationship with the individual.
6. **More Resources.** A federal privacy law should include increased funding authorization levels for the FTC to carry out its expanded obligations and better position itself to address healthcare privacy issues under such a framework.
7. **Rulemaking Authority.** Legislation should provide the FTC with limited, clearly defined Administrative Procedure Act rulemaking authority, enabling the FTC to define needed privacy and security guardrails where they are not already covered by existing laws (e.g., HIPAA and HITECH).

The App Association believes American Data Privacy and Protection Act (ADPPA, H.R. 8152, 117th Cong.) strikes a reasonable balance on several of its main provisions. I hope that my testimony has made it clear that modification of the existing laws at the expense of a national statute would lead only to additional complications. Congress should act on a strong, bipartisan, national framework for data privacy that draws from our evolving understanding of the needs of businesses and consumers.



U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

March 1, 2023

The Honorable Gus Bilirakis
Chair
Subcommittee on Innovation, Data
& Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data
& Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

In advance of your Subcommittee's hearing entitled "Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy," the U.S. Chamber of Commerce reiterates our support for a preemptive privacy standard that protects all Americans equally.

A Single National Privacy Standard

For the United States to continue to reap the benefits of the 21st century digital economy and enable a thriving ecosystem that facilitates small business growth, Congress must pass a single *preemptive* national privacy standard. Simply adopting a national privacy law without strong preemption would enable a state patchwork of laws that will be confusing to both consumers and potentially impossible for small businesses to comply.

A recent report from ITI highlighted that a national patchwork of privacy laws would cost the United States economy \$1 trillion and disproportionately impact small businesses with a \$200 billion economic burden.¹

To provide the strongest preemption, according to a Congressional Research Service report, Congress should use words like preemption "related to" certain subjects.²

Congress should avoid merely preempting what a proposed bill is "covering" or "covered by," because such clauses are considered by the Supreme Court to be less restrictive on states than phrases like "related to."³ According to the Supreme Court, "'Covering' is a more restrictive term which indicates that preemption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."⁴ A national privacy law that merely preempts what is "covers" and then provides for exceptions to that preemption would likely be taken by many as evidence that Congress has not intended to "substantially subsume" regulation.

¹ <https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/>.

² <https://crsreports.congress.gov/product/pdf/R/R45825>

³ *Id.* at 10.

⁴ *CSX Transportation, Inc. v. Easterwood*, 507 U.S. 663 (1993.)

In recent years, legislation has been authored by Republican and Democrats that would provide strong preemption:

- In the 117th Congress, H.R. 1816, the Information Transparency and Personal Data Control Act provided that, “No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard *related to* the data privacy or associated activities of covered entities.”⁵
- Also in the 117th Congress, Rep. Armstrong proposed an amendment to the American Data Privacy and Protection Act that would have provided, “No law, rule, regulation, requirement, prohibition, standard, or other provision having the force and effect of law *relating to* any subject matter regulated under this Act...”⁶
- In the 118th Congress, House Financial Services Committee Chairman Patrick McHenry has proposed the “Data Privacy Act of 2023,” which provides that legislation “supersedes any statute or rule of a State.”⁷

Balanced Enforcement

Compliance should be collaborative and reside with appropriate regulators and enforcers like the Federal Trade Commission (FTC) and state attorneys general and not the trial bar through the use of private rights of action.⁸

Agency Enforcement

FTC has historically been the agency with the expertise in data privacy matters in the federal government for companies not regulated by sectoral data protection laws. The Chamber believes that FTC remains the appropriate agency to continue to regulate and enforce data protection—but with appropriate guardrails.

In light of FTC Commissioner Christine Wilson’s recent resignation in protest, the Chamber has called for oversight of the Commission’s mismanagement and called for a moratorium on granting the agency further rulemaking authority until appropriate safeguards were placed upon the agency to protect due process.⁹

In particular, we call to your attention FTC’s recent Advanced Notice of Proposed Rulemaking in which it appears to replace Congress and develop comprehensive privacy rules. Former Commissioner Noah Phillips who dissented against the proposal stated what the privacy

⁵ <https://www.congress.gov/bill/117th-congress/house-bill/1816/text> (emphasis added)

⁶ <https://docs.house.gov/meetings/IF/IF17/20220623/114958/BILLS-117-8152-A000370-Amdt-6.pdf> (emphasis added).

⁷ https://financialservices.house.gov/uploadedfiles/glb_2023_xml_2.24_934.pdf

⁸ https://www.uschamber.com/assets/archived/images/9.6.18_us_chamber_-_ctec_privacy_principles.pdf

⁹ https://www.uschamber.com/assets/documents/230216_FTC-Oversight_Sen.-CST-House-EC.pdf

rulemaking “does accomplish is to recast the Commission as a legislature, with virtually limitless rulemaking authority where personal data are concerned.”¹⁰

We believe FTC’s actions to exceed its authority run afoul of the Supreme Court’s “Major Questions Doctrine,” which holds that in matters of “political and economic significance” Congress must grant clear authority to an agency to regulate.¹¹

The Commission is subject to rulemaking requirements under the Magnuson-Moss Act regarding its mandate to enforce against “unfair and deceptive trade practices.”¹² The Magnuson Moss Act did not delegate authority to the FTC but imposed heightened procedural safeguards on the agency. Knowing the FTC is flouting the procedural constraints placed upon it, Congress should not delegate broad new rulemaking authority to the Federal Trade Commission.

For example, Congress should refrain from granting the Commission Administrative Procedure Act-style rulemaking authority to broadly define types of data that are prohibited from collection without exceptions like consumer consent. If the Commission were to determine that broad categories of data are prohibited from collection it would be harmful to small businesses. According to a recent report from the Chamber, **80 percent** of small businesses stated that technology platforms like payments apps, digital advertising, and delivery help them compete with larger companies.¹³ **80 percent** of small business also say that limiting access to data will harm their business operations.¹⁴ One small business owner of a coffee shop stated in response to the FTC being able to have this kind of authority said¹⁵:

This is very unfortunate as it would essentially be another “pandemic” for us. Not having customer data means that we would go back to the early 1980’s where we would market our products to a generic list, which in turn would be extremely costly and not a good customer experience. Having customer data helps us customize our marketing so the end result is more meaningful to the customer.

The Commission should narrowly tailor rulemaking authorities that it gives the Federal Trade Commission.

Private Rights of Action

¹⁰

https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf

¹¹ https://www.uschamber.com/assets/documents/221121_Comments_CommercialSurveillanceDataSecurity_FTC.pdf

¹² 15 U.S.C. § 45.

¹³ <https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf>

¹⁴ *Id.*

¹⁵ <https://www.uschamber.com/technology/small-business-owners-credit-technology-platforms-as-a-lifeline-for-their-business> (emphasis added).

Comprehensive privacy legislation should leave enforcement to agencies like the Federal Trade Commission and state attorneys general and not empower the private trial bar at the expense of business innovation and viability. Frivolous, non-harm-based litigation in particular has been used in the past to extract costly settlements from companies, even small businesses, based on privacy law provisions granting a private right of action. Private rights of action are ill-suited in privacy laws because:¹⁶

- Private rights of action undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who can be expected to understand the complexities of encouraging compliance and innovation while preventing and remediating harms.
- They can also lead to a series of inconsistent and dramatically varied, district-by-district court rulings. Agency enforcement can provide constructive, consistent decisions that shape privacy protections for all American consumers and provide structure for companies aiming to align their practices with existing and developing law.
- Combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, private rights of action are routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionately benefit plaintiffs' lawyers rather than individuals whose privacy interests may have been infringed.
- They also hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technologies.

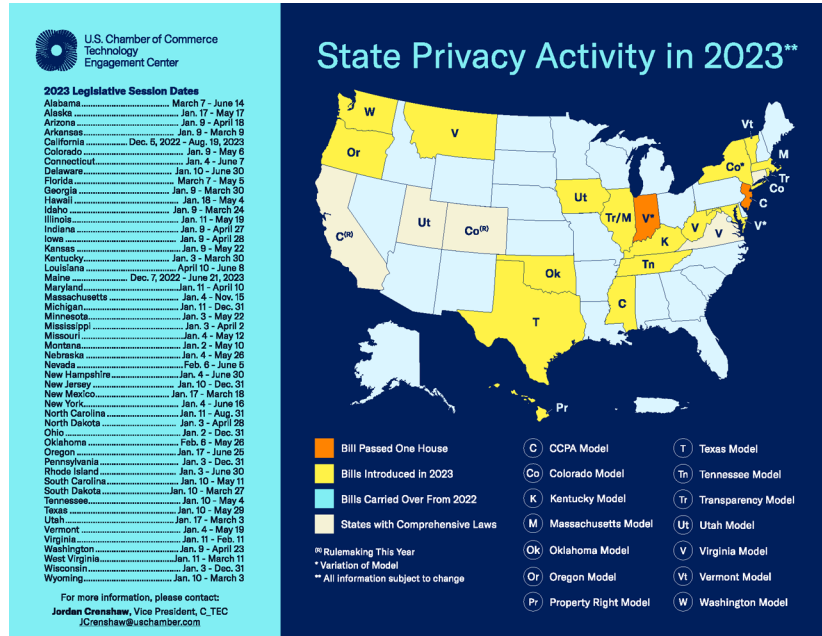
Private rights of action would be particularly devastating for business under a privacy law that does not have a strong preemptive effect. Not only would states be able to continue passing their own laws, but individual judicial district precedent could also create further confusion and conflict.

Harmonizing State Trends

Congress should incorporate principles from good state legislation into a national privacy law because companies are already operationalizing requirements in five states. It has been more than 1,700 days since the California Consumer Privacy Act (CCPA) was signed into law. Since then, four other states have passed comprehensive privacy laws and another 20 are considering their own bills. The map provided below¹⁷ illustrates that states are looking at diverging privacy proposals which further emphasizes the need for a preemptive national privacy standard.

¹⁶ [https://institutelegalreform.com/wp-content/uploads/2020/10/III-Suited - Private Rights of Action and Privacy Claims Report.pdf](https://institutelegalreform.com/wp-content/uploads/2020/10/III-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf)

¹⁷ For detailed summaries of the state proposals visit <https://americaninnovators.com/2023-data-privacy/>.



When framing a national privacy law, Congress should assess where trends are developing. For example, all state privacy laws that have been enacted provide some form of transparency requirement and grant consumers access, deletion, correction, and opt out rights in the case of things like data sales. No state privacy law has created a private right of action for privacy violations. Rather, these laws have granted state attorneys general or other relevant agencies enforcement powers. No state privacy law has strict opt-in or broad data collection prohibitions that as described above could harm small businesses. As a general trend, red and purple states like Texas, Indiana, Maryland, Iowa, and Montana are considering legislation that resemble variants of Virginia's new privacy law. Traditionally blue states are considering legislation that resembles either CCPA, the American Data Privacy and Protection Act, or strictly opt-in consent regimes with private rights of action.

Conclusion

It is urgent that Congress pass preemptive national privacy legislation that provides strong protections for all Americans equally. Additionally, agencies like the FTC should be given narrow

grants of authority with appropriate guardrails. Enforcement should not be exercised through private rights of action. We also urge Congress to build operational harmony into a national privacy law by drawing upon workable provisions of state privacy laws that protect consumers and provide certainty.

Sincerely,

A handwritten signature in black ink, reading "Jordan Crenshaw". The signature is written in a cursive, flowing style.

Jordan Crenshaw
Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

cc: House Energy & Commerce Committee



Robyn Boerstling

Vice President

Infrastructure, Innovation and Human Resources Policy

March 1, 2023

Representative Gus Bilirakis
Chair
Subcommittee on Consumer Protection
and Commerce
Committee on Energy and Commerce
Washington, DC 20515

Representative Janice Schakowsky
Ranking Member
Subcommittee on Consumer Protection
and Commerce
Committee on Energy and Commerce
Washington, DC 20515

Dear Chair Bilirakis and Ranking Member Schakowsky:

The National Association of Manufacturers welcomes the subcommittee's focus on data privacy. The NAM is the largest manufacturing association in the United States representing manufacturers in every industrial sector and in all 50 states. Manufacturing employs more than 13 million men and women, contributes nearly \$2.81 trillion to the U.S. economy annually, has one of the largest economic impacts of any major sector and accounts for 55% of all private-sector research and development in the nation.¹ The NAM is the powerful voice of the manufacturing community and the leading advocate for a policy agenda that helps manufacturers compete in the global economy and create jobs across the United States.

Today's hearing "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy" is an opportunity to further explore this important issue and assess the strong need for a federal data privacy standard. Manufacturers resoundingly support a federal data privacy standard that prevents a patchwork of state privacy laws and provides much needed legal clarity to support continued innovation and competitiveness.

Manufacturers are continuously developing innovative products and transforming the manufacturing process with the latest technologies. Data continues to be a critical source and byproduct of these breakthroughs and developments as modern manufacturing evolves. The Internet of Things (IoT) is continuing to transform manufacturing through billions of connected devices and advanced wireless infrastructure that allow for the transmission of vast amounts of data. Connected shop floors are generating data that industry is harnessing to improve efficiency, manage production activities, streamline repairs and safeguard plant security. Additionally, connected products utilize data to transform the consumers' experience in countless ways.

Our nation's manufacturers support ongoing efforts to craft federal data privacy legislation that advances individuals' privacy while promoting U.S. innovation and industrial competitiveness. Without clarity from federal law, uncertainty will continue for our industry, causing manufacturers to sort through conflicting state privacy laws across the country. To provide greater legal clarity, federal privacy legislation should pre-empt state privacy regulations

¹ <https://www.nam.org/facts-about-manufacturing/>

to resolve conflicting requirements in different states. A national approach to data privacy will strengthen businesses while supporting consumers.

Patchwork state privacy laws and unpredictable regulatory changes on data privacy are currently undermining the ability of organizations to manage privacy risks, protect consumers and make business decisions with the certainty they need. State-by-state privacy requirements create conflicts for manufacturers, their operations and their processes due to the interstate nature of data flows. They stall innovation by creating a regulatory burden that distracts from the development of next generation technologies and products. Manufacturers design and build security and privacy into their systems and products and it is often an extensive process to adjust those systems and products in the face of evolving data regulations.

Ongoing innovation requires flexibility, and any federal action on data privacy must be carefully balanced and thoughtfully implemented without sacrificing opportunities for economic leadership and progress. Businesses should be held accountable if they inappropriately utilize personal consumer data or violate a data privacy agreement. However, legislation that includes a private right of action should be constructed in a thoughtful way to prevent a legal dynamic that could encourage excessive legal challenges. Rather than innovating, companies could be focusing resources on unending legal challenges that the legislation unintentionally encourages.

Our companies are entrusted with vast amounts of data through diverse business interactions with customers, vendors, suppliers and governments. They understand that safeguarding privacy, protecting information and building consumer trust is a critical responsibility. Manufacturers support a data privacy policy that provides flexibility for innovation and advances U.S. economic growth and technological leadership. The NAM appreciates the work of the subcommittee and looks forward to engaging with you on this issue.

Sincerely,



Robyn M. Boerstling

Cc: Chair Cathy McMorris Rogers
U.S. House of Representatives
Committee on Energy and Commerce

Ranking Member Frank Pallone
U.S. House of Representatives
Committee on Energy and Commerce

**The Leadership Conference
on Civil and Human Rights**

1620 L Street, NW
Suite 1100
Washington, DC
20036
202.466.3311 voice
202.466.3435 fax
www.civilrights.org



February 28, 2023

Officers
Chair
Judith L. Lichman
National Partnership for
Women & Families
Vice Chairs
Margaret Huang
Southern Poverty Law Center
Derrick Johnson
NAACP
Thomas A. Saenz
Mexican American Legal
Defense and Educational Fund
Secretary
Palma Goss Graves
National Women's Law Center
Treasurer
Lee A. Saunders
American Federation of State,
County and Municipal Employees

Board of Directors
Abel Ayoub
American-Arab
Anti-Discrimination Committee
Gloria L. Blackwell
AAUW
Ray Curry
International Union, UAW
Jocelyn Frye
National Partnership for
Women & Families
Jonathan Greenblatt
Anti-Defamation League
Mary Kay Henry
Service Employees International Union
Damon Hewitt
Lawyers' Committee for
Civil Rights Under Law
David H. Inoue
Japanese American Citizens League
Virginia Kass Solomon
League of Women Voters of the
United States
Marc Morial
National Urban League
Janet Murguia
UnidosUS
Svenette Myrick
People For the American Way
Jenai Nelson
NAACP Legal Defense and
Educational Fund, Inc.
Christian F. Nunes
National Organization for Women
Rabbi Jonah Pesner
Religious Action Center
of Reform Judaism
Rebecca Pingle
National Education Association
Lisa Rice
National Fair Housing Alliance
Kelley Robinson
Human Rights Campaign
Anthony Romero
American Civil Liberties Union
Liz Shuler
AFL-CIO
Fawn Sharp
National Congress of American Indians
Maria Town
American Association of
People with Disabilities
Randi Weingarten
American Federation of Teachers
John C. Yang
Asian Americans Advancing Justice |
AAJC

President and CEO
Maya Wiley

**The Honorable Cathy McMorris
Rodgers**
Chair
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Gus Bilirakis
Chair
Subcommittee on Innovation, Data, and Commerce
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chair McMorris Rodgers, Ranking Member Pallone, Chair Bilirakis, and Ranking Member Schakowsky,

On behalf of The Leadership Conference on Civil and Human Rights, a coalition charged by its diverse membership of more than 230 national organizations to promote and protect the rights of all persons in the United States, we thank you for the opportunity to submit our views regarding online privacy. We ask for this letter to be entered into the record of the Innovation, Data, and Commerce Subcommittee hearing titled "Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy" on March 1, 2023.

Technological progress should bring greater safety, economic opportunity, and convenience to everyone. And the collection of demographic data is essential for documenting persistent inequality and discrimination. But just as technology has created immense positive value by creating economic opportunities, facilitating civil rights advocacy, and adding new voices to our culture and public debate, it can also enable discriminatory conduct and give new tools to powerful institutions to entrench and exacerbate existing disparities. In 2014, The Leadership Conference, along with 14 signatories, released the "Civil Rights Principles for the Era of Big Data," (civil rights principles) calling on the U.S. government and businesses to respect and promote equal opportunity and equal justice in the development and use of data-driven technologies.¹ While the terminology has shifted from "big data" to "AI," the issues remain the same and the threats technology can pose to civil rights have only grown.

¹ "Civil Rights Principles for the Era of Big Data," The Leadership Conference on Civil and Human Rights (Feb. 27, 2014), <https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/#:~:text=Technological%20progress%20should%20bring%20greater,documenting%20persistent%20inequality%20and%20discrimination.>



Recognizing this increased urgency, as well as the growing disparity between the vast amount of personal data available to companies, and the tiny amount of information available to the public about how companies are using it, in 2020, The Leadership Conference, along with a number of advocacy and civil rights organizations, released updated civil rights principles.² Those principles include ending high tech profiling; ensuring justice in automated decisions; preserving constitutional principles; ensuring that technology serves people historically subject to discrimination; defining responsible use of personal information and enhancing individual rights; and making systems transparent and accountable.

Today, tens of millions of people are without any kind of legal protections for their personal data.³ They are discriminated against in housing, employment, credit, education, finance, and other economic opportunities, and they are left in the dark about how their personal data is used.⁴ As we have told this committee on multiple occasions, privacy rights are civil rights.⁵ Well-drafted comprehensive federal consumer privacy legislation like the American Data Privacy and Protection Act (ADPPA) introduced in the last Congress will protect civil and human rights; empower communities of color; ensure opportunities are open for marginalized populations; and ensure that companies, including “Big Tech,” are held accountable for the data they collect and use, especially when those actions impact individuals’ lives.

The ADPPA, as it was voted out of the committee last Congress, contained important provisions that served to address these issues. The legislation prohibited the use of personal data in a discriminatory manner in the provision of goods or services on the basis of protected characteristics and ensured that these protections would be incorporated into the sectors that need them most through requirements to test algorithms for bias and measure potential impacts on equal access to and eligibility for housing, employment, credit, education, insurance, health care, and public accommodations. It also preserved state civil rights laws and other types of state laws that are important for the protection of consumers and marginalized communities. Strong data minimization requirements found in ADPPA further protected the rights of individuals by limiting potential data surveillance.

Under the bill, consumers would have been able to hold companies accountable for data misuse through a private right of action. The Federal Trade Commission was given enforcement authority, and attorneys general and privacy agencies in every state in the country were empowered to enforce ADPPA. Through

² Press Release, “Civil Rights Leaders Announce Principles to Protect Civil Rights and Technology,” The Leadership Conference on Civil and Human Rights (Oct. 21, 2020), <https://civilrights.org/2020/10/21/civil-rights-leaders-announce-principles-to-protect-civil-rights-and-technology/>.

³ Thorin Klosowski, “The State of Consumer Data Privacy Laws in the US (And Why It Matters),” N.Y. Times (Sept. 6, 2021), <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>.

⁴ “The Leadership Conference on Civil and Human Rights Views on Discussion Draft of The American Data and Privacy Act,” The Leadership Conference on Civil and Human Rights (June 14, 2022), <https://civilrights.org/resource/letter-to-house-energy-and-commerce-committee-on-the-american-data-privacy-and-protection-act/>.

⁵ “The Leadership Conference on Civil and Human Rights Views on Discussion Draft of The American Data and Privacy Act,” The Leadership Conference on Civil and Human Rights (June 14, 2022), <https://civilrights.org/resource/letter-to-house-energy-and-commerce-committee-on-the-american-data-privacy-and-protection-act/>.

February 28, 2023
Page 3 of 3



these three layers of enforcement, consumers and our institutions would have been able to effectuate meaningful change and hold bad actors accountable.

These provisions are a key reason why The Leadership Conference endorsed the ADPPA. Any privacy legislation moving forward must include a prohibition on the use of personal data in a discriminatory manner in the provision of goods or services on the basis of protected characteristics, the preservation of state civil rights laws and other types of state laws important for the protection of consumers, data minimization requirements, a private right of action, and enforcement authority across the federal government and state governments.

We stand ready to work with Congress on policies that will protect civil rights, prevent unlawful discrimination, and advance equal opportunity. Should you require further information or have any questions regarding this issue, please feel free to contact Jonathan Walter, media and tech policy counsel, at walter@civilrights.org, Frank Torres, civil rights technology fellow, at torres@civilrights.org, or Anita Banerji, senior director of the media and tech program, at banerji@civilrights.org.

Sincerely,

Jesselyn McCurdy
Executive Vice President of Government Affairs



September 26, 2022

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Kevin McCarthy
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Chairman
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jan Schakowsky
Chairwoman
Consumer Protection &
Commerce Subcommittee
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Gus Bilirakis
Ranking Member
Consumer Protection &
Commerce Subcommittee
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Speaker Pelosi, Leader McCarthy, Chairman Pallone, Ranking Member McMorris Rodgers, Chairwoman Schakowsky, and Ranking Member Bilirakis:

We write to express deep concern about significant public safety consequences that could result if the American Data Privacy Protection Act (ADPPA, H.R. 8152) were to be enacted as currently drafted. Data privacy protections are critical for the safety of our citizens and our national security. Law enforcement also has a vested interest in data privacy as it directly relates to officer safety. Many law enforcement agencies have seen officers' personal data publicly exposed, and these officers and their families have been harassed and threatened as a result.

While strong consumer data privacy protections are needed, the ADPPA in its current form would likely have major negative consequences that would make it harder to investigate criminal activity. For example, in its current form, the ADPPA would likely complicate the private sector's ability to continue its ongoing efforts to cooperate and voluntarily share certain information with law enforcement throughout the course of a criminal investigation.

This legislation would also make common investigative tools unavailable or extremely limited. These tools are used successfully by law enforcement agencies around the country every day to investigate violent crime, human trafficking, child sexual exploitation, fentanyl and opioids trafficking, violent extremism, carjacking, kidnapping, and threats of mass violence that are made on social media. These tools provide the essential building blocks for generating leads, especially in the early stages of a critical incident, and there is simply nothing that can replace that capability for investigators. Some have grossly misconstrued how law enforcement uses these investigative tools to justify their elimination via the ADPPA. The reality is that law enforcement agencies have strict policies and procedures in place to mitigate the risk of misuse and abuse.

At a time when Congress is working to pass laws that support effective and accountable law enforcement and reduce violent crime, the ADPPA in its current form would make our jobs harder. It is a 21st Century reality that digital information generated by public and private entities is relevant to most criminal investigations. The ADPPA prevents law enforcement from obtaining publicly available information in a timely, lawful manner, which significantly jeopardizes our ability to rescue victims, protect communities, and prevent bad actors from exacerbating an already historic rise in violent crime. As currently written, this bill will make it more difficult for law enforcement to find critical pieces of information that are necessary to quickly generate leads and solve crimes.

Congress cannot push law enforcement's investigative capabilities back into the 20th Century as we try to address today's 21st Century criminal challenges. We strongly oppose the current version of ADPPA and urge the House to improve the bill to protect consumer privacy without weakening criminal investigations. Our organizations stand ready to work with you to achieve this balance.

Sincerely,

Association of State Criminal Investigative Agencies (ASCIA)
 Federal Law Enforcement Officers Association (FLEOA)
 Major Cities Chiefs Association (MCCA)
 Major Count Sheriffs of America (MCSA)
 National Association of Assistant U.S. Attorneys (NAAUSA)
 National Association of Police Organizations (NAPO)
 National District Attorneys Association (NDAA)
 National Fusion Center Association (NFCA)
 National Narcotics Officers' Associations' Coalition (NNOAC)
 Sergeants Benevolent Association (SBA)



September 26, 2022

The Honorable Nancy P. Pelosi
Speaker of the House
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Kevin O. McCarthy
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank J. Pallone Jr.
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Cathy A. McMorris Rodgers
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Madam Speaker, Mr. Chairman, and Representatives McCarthy and McMorris Rodgers,

We are writing on behalf of the Fraternal Order of Police (FOP) and the International Association of Chiefs of Police (IACP) to raise our serious concerns with current provisions in H.R. 8152, the "American Data Privacy Protection Act." Our organizations strongly support data privacy for all Americans. It is particularly critical to the safety of our officers whose personal information, if compromised, could put them and their families in jeopardy. However, we must be sure that we protect this personal data without negatively impacting the ability of law enforcement to conduct routine investigations.

Consumer data privacy protections are very important in this digital age, but in protecting personal data from unauthorized or unlawful access, we must be sure not to make it more difficult for law enforcement to conduct criminal investigations by accessing publicly available information from private sector entities who want to cooperate with law enforcement and voluntarily share information to assist in criminal investigations.

There are provisions in the bill as introduced that will negatively impact investigations by law enforcement and render many of the common tools these agencies currently use unavailable or too limited. Law enforcement agencies pursuing investigations into violent crimes like human trafficking, child exploitation, kidnapping, or threats of mass violence need these tools to generate leads and prevent potential harm to our citizens. For example, in the early hours following an abduction, access to publicly available data and the tools to quickly and efficiently search for this information is of the utmost importance to avoid tragic outcomes.

We live in a world of digital data and all of our lives are increasingly intertwined as we interact in publicly available virtual space. Because of this, law enforcement officers must be able to obtain publicly available information quickly and lawfully in order to protect the public, rescue victims, solve crimes, and prevent

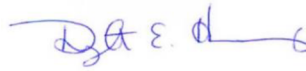
criminal actors from escaping justice. This legislation, as currently drafted, would jeopardize law enforcement's ability to do its job and it will put lives at risk.

On behalf of the members of the FOP and the IACP, the largest and most prominent labor and management law enforcement organizations in the country, we urge the House to work with law enforcement and public safety-oriented stakeholders to make the necessary changes to the legislation in order to preserve our ability to conduct effective investigations and protect our personal data.

Sincerely,

A handwritten signature in black ink, appearing to read "Patrick Yoes", with a stylized flourish at the end.

Patrick Yoes
National FOP President

A handwritten signature in blue ink, appearing to read "Dwight Henninger", with a stylized flourish at the end.

Chief Dwight Henninger
IACP President



WRITTEN RESPONSES – QUESTIONS FOR THE RECORD
Graham Mudd
President & Chief Product Officer
Anonym, Inc

FOR THE
Subcommittee on Innovation, Data, and Commerce
Committee on Energy & Commerce
United States House of Representatives

HEARING ON
Promoting U.S. Innovation And Individual Liberty Through
A National Standard For Data Privacy
March 1, 2023

Attachment 1—Additional Questions for the Record**The Honorable Diana Harshbarger**

As more and more connected technology devices are increasingly tracking human behavior and producing more and more data, do you think consumers should have ownership over this data?

Yes, I do believe that consumers should have more ownership and control over the data they generate – and that this issue will only become more important as Americans’ use and reliance on connected devices deepens. Unlike physical property, data is infinitely replicable, which means it can be reproduced and shared with additional parties at very little cost. This means consumers can very quickly and easily lose any measure of control over their data. Without federal legislation in place, consumers have little assurance that data they generate and share with one party won’t be shared with others and put to use in ways that may harm them. For example, in the digital advertising industry, data is a powerful asset, so there is a strong incentive for companies to share data with the platforms through which they advertise. As a result, advertising technology companies and data brokers build and maintain incredibly deep profiles of people’ online and real-world behavior. These profiles can be used in ways that are counter to an individual’s interests.

The Honorable Russ Fulcher

I wanted to ask you about the importance of ensuring the ability for businesses to continue to innovate. I want to give you more time to address the question below.

In the years since GDPR went into effect, we have seen the fall out in the EU. Large businesses continue to grow larger while small businesses and startups are becoming a rarity.

1. How can we ensure this does not happen within the United States?

Many would argue that GDPR was overly burdensome to small businesses, particularly relative to the potential privacy harms that these businesses are capable of inflicting. There are a number of potential lessons that can be drawn from GDPR, many of which are already addressed in the latest draft of ADPPA.

For example, the most significant compliance requirements should be focused on the entities whose data practices have the potential to affect the greatest harm. Data volume is one dimension to consider. For example, entities that collect data from many other companies to develop consolidated profiles on millions of individuals are worthy of more regulatory focus than small businesses who maintain information on a modest customer base.

The sensitivity of the data handled by an entity is another dimension to consider. Companies that handle health or financial information should reasonably be subject to stricter compliance requirements than businesses that handle de-identified or less sensitive data.

ADPPA recognizes both of these dimensions and requires more of companies that handle either large volumes of data or sensitive data than those which do not. For example, small businesses, as defined by

ADPPA, are exempt from requirements to provide consumers with the right to request or correct their data, and from the requirement to establish a data privacy or security officer.

It's also important to proactively support small businesses in their compliance efforts. The ADPPA requires the FTC to develop a compliance program – this program should devote considerable resources to supporting small businesses.

In addition, Congress and regulatory agencies should encourage the development of technologies that support the adoption of privacy preserving practices (sometimes called "privacy-enhancing technologies," a.k.a. "PETs"). This can make privacy compliance easier for small businesses that don't have deep in-house privacy expertise. It also can level the playing field for small businesses that want to leverage data for analysis without compromising customers' privacy.

Thank you for your expertise. I know that the digital ecosystem runs on information, but sometimes it seems companies and data brokers are collecting more information than they need.

2. *Can you explain what information companies are collecting, what information they are using, and if they aren't using everything, why collect more information than they are actually using?*

It's difficult to answer your question about what is collected other than to say "everything." If a given behavior or attribute is digitally observable, then it is more than likely collected.

Without regulations in place, it is often the case that there are strong incentives to collect more information than might be immediately or obviously useful. This is because collecting and storing information is typically extremely inexpensive and unforeseen new applications for already-collected data are likely to arise in the future. For example, machine learning can be used to discover correlations that help a business make a prediction about consumer behavior that are far from obvious to humans.

Data minimization requirements, such as those included in ADPPA, provide a necessary incentive to reduce the collection, storage and transfer of data that isn't strictly necessary for an allowed purpose. These requirements can, and should, encourage companies to de-identify and anonymize data, which meaningfully reduces privacy risks while still supporting most applications and uses.



Jessica Herron
Clerk, Innovation, Data, and Commerce
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515
Via email

Wednesday March 29, 2023

Re: QFR Responses for Hearing Entitled “Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy”, March 1, 2023.

Dear Ms. Herron:

Thank you for the invitation to appear before the Subcommittee on Innovation, Data & Commerce to testify during the March 1, 2023 hearing entitled “Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy.”

Pursuant to the Committee’s Rules, I have been asked to answer an additional question for the record, my response to which is attached.

Sincerely,

A handwritten signature in black ink, reading "Alexandra Reeve Givens". The signature is fluid and cursive, with the first name "Alexandra" being the most prominent.

Alexandra Reeve Givens

Written Responses - Question for the Record
Alexandra Reeve Givens
President & CEO, Center for Democracy & Technology

For the U.S. House of Representatives Energy & Commerce Committee,
Subcommittee on Innovation, Data, & Commerce
Hearing Entitled "Promoting U.S. Innovation and Individual
Liberty through a National Standard for Data Privacy"
March 1, 2023

The Honorable Diana Harshbarger

Question: As more and more connected technology devices are increasingly tracking human behavior and producing more and more data, do you think consumers should have ownership over this data?

Data ownership, while appealing in theory, is difficult to operationalize. One of the complicating factors is that data is a "non-rivalrous" good: copies of the same data can exist in multiple locations and be accessible by multiple people or entities, without necessarily jeopardizing each one's ability to make use of the data. For non-rivalrous goods, a property framework may not always be the best answer, particularly given how easy it is to copy data online. Further, allowing people to sell their data would benefit only the biggest online players, as large companies like Meta and Alphabet can surely afford to purchase the rights to use people's data from their significant user bases, while smaller start-ups would find that more difficult. And last, there is no guarantee that any particular piece of data would be worth more than a negligible amount, so it is unlikely that people would be compensated in a meaningful way. Large datasets are valuable because they allow for statistical analysis yielding insights about people or groups of people, but each individual data point, on its own, may not be worth much.

A more effective approach is to give people rights over data that pertains to them: rights to access, delete, correct, and port that data. These rights give people the ability to know what companies collect about them, and have the ability to correct it if it's wrong, delete it if they no longer want the company to have it, or port the data to another service provider. These rights have more meaning and value than the ability to own and sell data for fractions of a penny. They must, however, be enforceable, which is why a private right of action is such an important component of any federal privacy law (since the FTC and State Attorneys General are unlikely to prioritize these issues over other enforcement priorities).

However, the most important protections in any federal privacy law are data minimization and purpose limitation: prohibiting businesses and other entities from collecting more data than what is necessary to provide the service a person has requested. For example, an online retailer needs to collect customers' shipping information, payment details, contact information, and details about the product being sold. It does not need detailed demographic information about

the customer or data about other websites they have browsed, and should not collect and retain that data (let alone share or sell it to unknown third parties, as can happen now).

To expand on this point, our hypothetical online retailer should not be allowed to sell its customers' purchase records to a data broker, which might then combine all of a person's purchase records, aggregated from various retailers, and any other information the broker can amass including location and demographic data, to create a detailed dossier of someone's online and offline life. Such a record is likely to reveal sensitive information about that person's likes and dislikes, health conditions, political opinions, religious affiliation, and more. When such records can be sold on the open market to any willing buyer (including large tech companies and foreign governments), they are ripe for exploitation and abuse. A data ownership framework is unlikely to meaningfully address these harms, but a robust federal law prohibiting such data practices can give consumers the protections they need.



March 31, 2023

Jessica Herron
Legislative Clerk
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Re: Jessica L. Rich's Responses to Additional Questions for the Record

Dear Ms. Herron:

I want to thank the Subcommittee for inviting me to appear before it on March 1, 2023 to testify on the topic of "Promoting U.S. Innovation and Individual Liberty Through a National Standard for Data Privacy." It was an honor to testify, and your assistance both before and after the hearing was especially helpful.

Pursuant to the Rules of the Committee on Energy and Commerce, I am attaching my answers to additional questions for the record, in the required format.

Thanks again for your help, and please let me know if you have any questions.

Sincerely,

A handwritten signature in cursive script, appearing to read "JR", followed by a period.

Jessica Rich
Of Counsel and Senior Policy Advisor for Consumer Protection
Kelley Drye & Warren LLP

Attachment 1—Additional Questions for the RecordThe Honorable Diana Harshbarger

As more and more connected technology devices are increasingly tracking human behavior and producing more and more data, do you think consumers should have ownership over this data?

In theory, yes, consumers should own and control their data because of the adverse consequences that can result when that data is misused. However, one problem with an ownership model is that it would likely impose enormous burdens on consumers to manage their data and their privacy, including in each interaction they have with hundreds of companies. This could become completely unworkable, as we have learned from our experience with the notice-and-choice model for privacy. Indeed, the notice-and-choice model, while designed to give consumers more control over their data, ends up overwhelming them with hundreds of long and confusing privacy notices.

That's why there is so much support for the bipartisan ADPPA, which seeks to reduce these burdens on consumers and instead impose more duties on companies to follow responsible data practices, such as the duty to conduct privacy impact assessments; the duty not to discriminate; and restrictions on the use of sensitive data.

The Honorable Russ Fulcher

Building on our discussion in the hearing and specific to the American Data Privacy and Protection Act. In that act, certain entities are required to submit impact assessments to the FTC related to algorithms.

- 1. Currently, does the FTC have the ability to request information that would be included in the impact assessments using their own authority and also permit entities to submit such information in a manner that doesn't expose trade secrets?**

Yes, the FTC has the authority to request a wide range of information (under the [FTC Act](#) and the FTC's [Rules of Practice](#)) in order to determine whether there have been law violations. The FTC also has the authority to conduct studies, such as the one it is current conducting on [Pharmacy Benefit Managers \(PBMs\)](#).

Many of these investigations and studies involve sensitive information and trade secrets, including (in addition to the PBM study) investigations and studies regarding merger and other antitrust issues; data security and privacy; and health products and health claims. The law and FTC rules allow companies to mark information as "confidential" (such as when it involves trade secrets) so that it receive special treatment and confidential handling. See [here](#) for a summary.

How would the FTC handle receiving all of these impact assessments if companies would be required to submit every assessment versus the FTC asking for it on their own accord?

Currently, the FTC obtains and reviews many third-party assessments, pursuant to its privacy and data security orders. While some of these assessments are automatically submitted to the agency, others are obtained by the FTC on request. In my experience, the FTC *does* frequently ask for and review even those assessments that aren't automatically submitted. Nevertheless, the assessment requirements under the ADPPA, which apply to any entity meeting a certain size threshold and not just those under an FTC order, would significantly add to the FTC's duties here. For the FTC to perform this work effectively, it would require more resources.

I wanted to ask you about the importance of ensuring the ability for businesses to continue to innovate. I want to give you more time to address the question below.

In the years since GDPR went into effect, we have seen the fall out in the EU. Large businesses continue to grow larger while small businesses and startups are becoming a rarity.

2. How can we ensure this does not happen within the United States?

Innovation is a hallmark of the US economy, and any privacy law enacted in this country should ensure that innovation continues to flourish. By necessity, that includes ensuring that small businesses can continue to compete and serve their communities.

One part of the solution is enacting a federal privacy law that sets a consistent standard, rather than forcing companies to navigate and develop costly compliance schemes for multiple different state laws. While compromise on preemption seems necessary in order to pass a federal law, the law still should try to achieve as much consistency as possible.

Another part of the solution is to limit the compliance costs on small businesses. Indeed, many existing privacy laws actually favor large companies, due to the high cost of compliance or because they focus unduly on limiting data-sharing with third parties (something large companies can avoid by keeping their functions in-house). The ADPPA attempts to avoid these effects by placing less emphasis on third-party sharing (in favor of more even-handed restrictions on data misuse) and by scaling down some of the duties for small businesses. For example, the bill reduces the burdens on small businesses when it comes to the data portability and correction, data security, executive responsibility, and audit and assessment requirements.

