This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

RPTR SCHOETTLE

EDTR ZAMORA

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, D.C.

The subcommittee met, pursuant to call, at 8:34 a.m., in Room 2123, Rayburn House Office Building, Hon. Gus Bilirakis [chairman of the subcommittee] presiding.

Present: Representatives Bilirakis, Bucshon, Walberg, Duncan, Dunn, Lesko, Pence, Armstrong, Allen, Fulcher, Harshbarger, Cammack, Rodgers (ex officio), Schakowsky, 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, Consumer Protections & Commerce; Jessica Herron, Clerk, CPAC; Nate Hodson, Staff Director; Tara Hupman, Chief Counsel; Peter Kielty, General

Counsel; Emily King, Member Services Director; Tim Kurth, Chief Counsel, CPAC; Brannon Rains, Professional Staff Member, CPAC; 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.

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 chair now recognizes the subcommittee ranking member, Ms. Schakowsky, for her 5 minutes for an opening statement. Good morning.

[The prepared statement of Mr. Bilirakis follows:]

******** COMMITTEE INSERT ********

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 evermore 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 INSERT ********

Mr. Bilirakis. I thank the ranking member.

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

The Chair. 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 much 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 techs' 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 American's 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 Chair Rodgers follows:]

******** COMMITTEE INSERT ********

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.

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 consumers 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 INSERT ********

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, 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 CEO, 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 aggressive 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:]

******** COMMITTEE INSERT ********

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 my 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 hyper-target 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 labyrinths in 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 admiral 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:]

******** COMMITTEE INSERT ********

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, rule makings 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 privacy right of action.

Thank you very much. I look forward to your questions.

[The prepared statement of Ms. Rich follows:]

******** COMMITTEE INSERT ********

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 consumer 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 than 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. Yeah. 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.

Okay. 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 seat, and

even grandparents back in the driver 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. Okay. 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. Yeah, yeah. 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. Okay. 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 insights, 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, yeah.

Ms. Givens. Yeah. 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 America 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 is 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 safeguards 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 rulemaking 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.

RPTR KERR

EDTR SECKMAN

[9:33 a.m.]

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 market place 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.

The Chair. That is right.

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

And I recognize you for 5 minutes. Thank you.

The Chair. 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.

The Chair. 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.

The Chair. 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 is 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.

The Chair. 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.

The Chair. 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 cites 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 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 provide 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. The 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 targeted 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 me 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 Ms. 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 400, 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 forty. 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, okay? 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, okay? 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. Okay. 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 hyper-target 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.

Okay. 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 five 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 increase 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 committees 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, Ms. 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 Rogers 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 resumes, 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.

RPTR SCHOETTLE

EDTR ZAMORA

[10:33 a.m.]

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 product 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.

Okay. 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.]

RPTR SCHOETTLE

EDTR ZAMORA

[11:26 a.m.]

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, okay, 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 -- yeah, the youngest pharmacist.

Mrs. Harshbarger. Yeah.

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. Okay. 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. Okay. Very good.

Ms. Rich. I would add one thing to what my splendid co-panelists 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 is 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. Okay. 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 statulatory 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. Okay. 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 is 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. Yeah.

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 follow-up 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. Okay.

Ms. Givens. Mr. Fulcher, if I may, there are provisions in the ADPPA that protects 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. Okay. 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. Yeah, 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.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Carter. Okay. 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 stymy innovation -- because I am concerned about freedom of

speech. I am concerned about stymying 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 restricted rules that would stymy 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 rulemaking, 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. Yeah. 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. Okay. 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 Teknek; 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, entitled "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 follows:]

******** COMMITTEE INSERT ********

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.

[The information follows:]

******** COMMITTEE INSERT ********

This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

[Whereupon, at 12:04 p.m., the subcommittee was adjourned.]