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

Diversified Reporting Services, Inc.
RPTS FREEMAN
HIF117170

ADDRESSING AMERICA'S DATA PRIVACY SHORTFALLS:
HOW A NATIONAL STANDARD FILLS GAPS TO PROTECT AMERICANS'
PERSONAL INFORMATION
THURSDAY, APRIL 27, 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 2:02 p.m. in 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, Blunt Rochester, Soto, Trahan, Clarke, and Pallone (ex officio).

Also present: Representatives Obernolte; and Eshoo.

Staff Present: Kate Arey, Digital Director; Michael Cameron, Professional Staff Member; Jessica Herron, Clerk; Nate Hodson, Staff Director; Tara Hupman, Chief Counsel; Sean Kelly, Press Secretary; Peter Kielty, General Counsel; Emily King, Member Services Director; Tim Kurth, Chief Counsel; Brannon Rains, Professional Staff Member; Lacey Strahm, Fellow; Teddy Tanzer, Senior Counsel; Hannah Anton, Minority Policy Analyst; 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; Lisa Hone, Minority Chief Counsel, Innovation, Data, and Commerce; Joe Orlando, Minority Junior Professional Staff Member.

*Mr. Bilirakis. The subcommittee will come to order. The chair recognizes himself for an opening statement.

Again, good afternoon and welcome to the 36th hearing the U.S. Congress has held on privacy and data security over the last five years. I am using a bit of math there from one of our previous witnesses. As for the Energy and Commerce Committee, this will be our sixth hearing in the 118th Congress. We have now examined in depth how a Federal data privacy and security law can make us more competitive with China.

While a Federal standard is needed to protect Americans and balance the needs of business, government, and civil society, what happens when malicious actors like TikTok and the CCP, through ByteDance, exploit access to data, where the FTC's lines of jurisdiction and authority are and how that interplays with the comprehensive privacy law, the role of data brokers, and the lack of consumer protections over one's data, and, finally, our hearing today, which will examine how consumers may not be covered by sector-specific laws in a way that is consistent with their expectations.

The fact is that the data privacy and security concerns permeate across multiple areas within Congress, even in seemingly unrelated topics, which highlights just how important it is for us to work together across the aisle and across Capitol Hill to protect the American people.

In today's hearing we will discuss sectoral data privacy regimes like the Financial Sectors Gramm-Leach-Bliley Act; and the Fair Credit Reporting Act; and the health care's -- health sector's Health Insurance Portability and Accountability Act, or HIPAA; the education sector's Family Education Rights and Privacy Act, FERPA; and of course, the Children's Online Privacy Protection Act, COPPA, which this subcommittee knows very well, and the gaps in coverage that a piecemeal, sector-specific approach has created for consumers.

We will hear from the witnesses about how these gray areas for Americans also result in risks and uncertainty that businesses could better avoid if we had clearer rules of the road. This only gets more complicated as 50 different states move towards their own data privacy laws, meaning an increasingly complicated and confusing landscape for consumers and for businesses.

Having clear rules in place will protect Americans, particularly our kids, as well as fuel innovation in the American marketplace. Sounds good to me.

Each of the witnesses has a unique story to tell when it comes to these gaps, but the challenges are the same: consumers think their data is protected, but the sector-specific law in place does not extend as far as consumers expect.

Mr. Codling, with REGO Payment Architectures, will discuss how it is possible to operate a payments infrastructure that has strong protections for children. REGO has filled the gaps that exist with the GLBA and COPPA by protecting all kids under 18. We appreciate that very much.

Ms. Vance, with the Public Interest Privacy Center, is a recognized expert in FERPA and kids privacy. She will speak about how current gaps exist in educational privacy and child-specific laws that a comprehensive privacy law would cover.

Thanks very much for being here.

Mr. Britan, with Salesforce, helps clients collect data in a way that is compliant with the Federal sectors -- sectoral laws and state privacy laws. His clients do business in every sector, and will speak to compliance burdens that the patchwork of state laws has created.

Thanks for being here.

Mr. Reed, with the App Association, will discuss how the piecemeal approach of state laws creates confusion for member companies. App Association members are regulated by all of the sector-specific laws, and must spend significant resources complying with all of the various state data privacy laws. That is so tough. It has got to be very difficult.

In closing, I want to thank all the witnesses for coming today. I also want to thank Chair Rodgers and the ranking member, Ranking Member Pallone, for all of the progress we have made so far, and the continued commitment to get this done -- we will get it done -- as well as Ranking Member Schakowsky, who has made this effort a true bipartisan partnership. Thank you so much.

[The prepared statement of Mr. Bilirakis follows:]

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

*Mr. Bilirakis. Lastly, I want to recognize and thank a valuable member of our team, whose last day is tomorrow and has served as a technology fellow on our subcommittee, on our staff for this past year -- we are really going to miss you, Lacey -- Lacey Strahm.

Lacey, your insights and contribution, particularly with the NIL to the team, have been invaluable over these past years. I really appreciate all your hard work. And don't be a stranger. We are going to miss you tremendously.

*Ms. Schakowsky. Let's give her a round --

*Mr. Bilirakis. Yes, why not?

[Applause.]

*Mr. Bilirakis. Hey, Lacey, second thoughts?

[Laughter.]

*Mr. Bilirakis. No? I wish you would stay, but I understand.

I look forward to hearing from our witnesses today on providing protections for Americans and certainty for businesses.

So with that I will now recognize the gentlelady from Illinois, Ms. Schakowsky, for her five minutes for an opening statement.

*Ms. Schakowsky. Thank you so much, Mr. Chairman. You know, you mentioned that we have been working in the subcommittee and the full committee for at least five years, talking about how are we going to protect consumers' data. And rather than things getting better, despite our being able to pass it out of the full committee, which was a tremendous achievement in a totally bipartisan way, I think consumers are increasingly, every day, concerned about their inability to protect their private information.

And you outlined some of the sectoral ways that consumers are supposedly protected but don't do the full job and don't fill the gaps. You mentioned health care, so -- and I am really anxious to hear about that, among other things, because I think, at first, when HIPAA was put into place, the idea that doctors and hospitals would not be able to share information, there weren't so many applications out there that went well beyond that, and opportunities to go beyond that. But now we know that there are all kinds of apps that collect information, and may share that, even sell that, about you and your health: one example of what we have to do.

You mentioned financial information. Now, you know, there were days where we just went to our banks, and we were pretty sure that that information wasn't going to be shared, and there were some protections. But we now know that there are retailers, for example, who have plenty of information when we do shopping online, and lots of our data, the -- that leads back to all of our financial information becomes available.

And then you also mentioned FERPA, which is -- I didn't actually know the acronym, but I am going to say it -- it is the Family Education Rights and Privacy Act. For our kids. Well, you would hope that all of our -- and we know that all of the information about our children isn't -- is not protected right now. And for example, the student data. But children who attend private schools, they are not going to find that their information is protected. We know that there are a number of educational apps that our kids and, even as parents, that we are connecting them to, that may have lots more information about our children than we want. And that is always a primary concern for members of these committee --

of this committee.

So I think I want to just conclude by going back to what we have already done. We have passed the American Data Privacy and Protection Act out of this committee, and it is time for us to return to that. If there are things that we still need to do, if we want to continue negotiations on various parts -- but we passed a really good bill, and it is that that we ought to build on, that we ought to move forward on so that all those gaps that are now in protecting consumers' information, the information they do not want stolen, sold, the manipulations that are happening right now to our kids online, ourselves online, we can address this right now and get going once again on the ADPPA legislation and move forward as quickly as we can.

[The prepared statement of Ms. Schakowsky follows:]

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

*Ms. Schakowsky. With that, I yield back, Mr. Chair.

*Mr. Bilirakis. Thanks so very much. I appreciate it. And we are going to make a good bill even better.

I now recognize the chair of the full committee, Mrs. Rodgers, for her five minutes for an opening statement.

*The Chair. Thank you, Mr. Chairman. Good afternoon and welcome.

This is our sixth privacy and data security hearing this year. It gives us another chance to discuss our efforts to enact a comprehensive national standard. Currently, there are sector-specific Federal statutes on the books to protect data, ranging from health care to financial to youth-oriented laws.

While preserving those laws, the American Data and Privacy Protection Act passed out of committee with near unanimous 53 to 2 vote, and it included many safeguards to ensure activities in these various sectors remain governed by the appropriate state and Federal regulators. Many of these laws were crafted in this very hearing room over the last 30 years. The level of innovation and competition that resulted since then is amazing, and it represents some of the greatest accomplishments in American history.

That said, these technologies come with challenges that must be addressed. These companies have developed tools that interact to track Americans both online and offline, and they are also using their data to manipulate what we see and what we think. This is especially true for children.

I am very proud of our work last Congress to pass ADPPA out of committee. It included the strongest privacy protections for kids online. These protections have support from several stakeholders as being stronger than any proposals from any other Federal or state laws or proposals to date. It would make it illegal to target advertising to children, and treats data about kids under 17 as sensitive. This means establishing higher barriers for the transfer of personal information.

This provision, along with the overarching data minimization provisions and the ability to delete personal information, will make it tougher for kids' personal identifiable information, like their physical location, to land in the hands of drug dealers, sex traffickers, and other evil actors attempting to find and track them.

It would also require assessments for how their algorithms amplify harmful content. This will keep them accountable for stories like the one reported by Bloomberg last week about Tiktok's algorithm continuing to push suicide content to vulnerable children.

Child privacy protection advocates, including many parent groups, are already on the record in support of a national data privacy standard. It is just one piece of protecting children online.

This is difficult to get right, but it is imperative that we do. Through many discussions with stakeholders, we determined that an underlying framework of protections must be strong and consistent, no matter the user, young or old. For this reason, any legislation to protect kids online must be rooted in a comprehensive national standard for data privacy and security to ensure there are broad protections. As long as there are regulatory gaps, companies will exploit them in order to monetize the data captured, and refuse to do more to shield children from bad actors like cyber bullies, sex predators, drug dealers, and others trying to do harm. This can't be allowed to continue.

I can't emphasize this enough: We need legislation like ours that protects children from having their information harvested, like geolocation data -- gives everyone the power to delete the information collected on them, and opt out of collection together -- altogether; provides greater transparency over the algorithms these companies use to manipulate and amplify the information we see; and requires assessments for how algorithms harm children.

Last week, we had a hearing with the Federal Trade Commission. We raised concerns about the direction of the agency related to the unilateral rulemaking efforts. I believe the FTC should be the preeminent data protection agency in the world, but it needs to be at the direction of Congress.

I appreciate the work of the people in this room to ensure that we get this legislation right. Our efforts have shown us that the single best way to protect Americans in today's digital ecosystem is with a national privacy and data security standard, and the American people agree. More than 80 percent of Americans say that they are looking for Congress to act. It is our responsibility to ensure their data privacy and security, and to even higher levels of protections for their kids. It is time to rein in Big Tech.

[The prepared statement of The Chair follows:]

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

*The Chair. I look forward to your testimony, and I yield back.

*Mr. Bilirakis. Thank you very much, Madam Chair. And now I recognize the gentleman from New Jersey, Mr. Pallone, for five minutes for an opening statement.

*Mr. Pallone. Thank you, Chairman Bilirakis.

For decades we have sought to safeguard Americans' fundamental right to privacy with a series of fragmented sector-by-sector laws. Anyone with a smartphone, laptop, or tablet can tell you that we are not getting the job done. The alphabet soup of well-intentioned Federal privacy laws HIPAA, COPPA, FERPA, GLBA have failed to rein in the collection, use, and transfer of Americans' sensitive data. That is partly because they were not designed for our modern online economy.

FERPA, or the Federal Educational Rights and Privacy Act, passed in 1974; HIPAA, or the Health Insurance Portability Accountability Act passed in 1996; GLBA, or the Gramm-Leach-Bliley Act, which addresses privacy within the financial sector passed in 1999; and COPPA, or the Children's Online Privacy Protection Act, became law in 2000. So the phone wasn't released -- or I should say that the iPhone wasn't released until 2007. In Internet years, these laws are dinosaurs.

So today health information is no longer confined to the relative safety of a doctor's filing cabinet. Fitness trackers monitor our heart rates, sleep patterns, and oxygen saturation levels. Health information websites provide diagnosis and treatment information on every possible medical condition. Mobile applications track dietary, mental, and reproductive health. But the HIPAA privacy rules only restrict the use and sharing of health information by health care providers, clearinghouses, and health plans. As a result, some of the most commonly-used websites, apps, and devices have the green light to mine and use Americans' health information without meaningful limitations.

The lack of strong privacy protections threatens Americans financial information, as well. Existing financial privacy laws largely do not apply to retailers and online marketplaces, nor do they provide protection from discriminatory algorithms.

Likewise, existing children's privacy laws leave vast amounts of children and teens' sensitive information unprotected. FERPA, the privacy law protecting educational records, does not apply to private and parochial elementary and secondary schools. It also doesn't apply to EdTech downloaded and used at home or in after-school programs to supplement or complement children's schoolwork. And COPPA only restricts online operators from collecting data from children under the age of 13 without obtaining verifiable parental consent, but only under limited circumstances.

Children's data collected on sites like TikTok, Instagram, Google, Facebook, and Snapchat is not protected unless the site knows it is collecting information from kids under 13. So this honor system has become a get-out-of-jail-free card for Big Tech companies, which often claim that their services are intended for users 13 or older. But we know children are on these sites and apps: 64 percent of children between 8 and 12 years old report watching online videos on platforms like TikTok and YouTube every day; nearly 1 in 5 say they use social media every day.

So simply tweaking current child privacy laws will not sufficiently protect our nation's youth. That is because age verification is notoriously challenging, and has proven to be ineffective. After all, children today are digital natives. They know how to bypass pop-ups asking for their age or birth date, and can enter these virtual playgrounds with little parental supervision and meager privacy protections.

So we also know that parents' use of the Internet routinely provides information about their children, either directly or by inference. When a parent or guardian goes online to research and sign up for summer camps, family vacations, little league teams, gymnastic classes, or a broad variety of other activities, they share data about their children, and that information is then used and shared for targeted marketing and other purposes. As a result, protecting kids and teens' privacy requires us to protect everyone's privacy.

So that is why we must pass a comprehensive privacy bill that closes the gap and enshrines Americans' right to privacy in law. We need a bill that reins in the over-collection of information by mandating data minimization. And we need a bill that puts all Americans back in control of how the data is collected, used, and shared.

Last Congress, as, you know, most of my colleagues have already mentioned, this committee overwhelmingly passed such a bill with broad bipartisan support. I am committed to getting a bill over the finish line, and look forward to continuing to work with Chair Rodgers and our subcommittee chairs to that effect.

[The prepared statement of Mr. Pallone follows:]

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

*Mr. Pallone. And with that, Mr. Chairman, I yield back. But thank you and Chair Rodgers and Ranking Member Schakowsky for all that you are doing to push this national privacy bill and framework. I appreciate it.

*Mr. Bilirakis. Good. Let's get this done. Now -- thank you very much, I appreciate it, the gentleman yields back.

Our first witness is Morgan Reed, president of ACT, the App Association.

You are recognized, sir, for your five minutes.

STATEMENT OF MORGAN REED, PRESIDENT, ACT, THE APP ASSOCIATION; DONALD CODLING, SENIOR ADVISOR FOR CYBERSECURITY AND PRIVACY, REGO PAYMENT ARCHITECTURES, INC.; EDWARD BRITAN, HEAD OF GLOBAL PRIVACY, SALESFORCE, INC.; AND AMELIA VANCE, FOUNDER AND PRESIDENT, PUBLIC INTEREST PRIVACY CENTER

STATEMENT OF MORGAN REED

*Mr. Reed. Chairman Bilirakis, Ranking Member Schakowsky, and members of the subcommittee, my name is Morgan Reed and I am the president of the App Association.

The App Association is part of a $1.8 trillion global ecosystem that supports 6 million American jobs. Our members are often tiny companies, but quite literally serve all 435 congressional districts. And most importantly, our member companies are building products that help your constituents manage their health, their finances, and their education.

For example, two companies -- Thinkamingo in your district, Mr. Chair; and Kidz Learn in your district, Ms. Schakowsky -- must manage the intersection between COPPA and FERPA and the gaps that exist. In health care our companies like Podimetrics help veteran warfighters manage their diabetic foot issues, and Rimidi gives doctors a platform to manage remote patient monitoring, all while dealing with HIPAA rules for both data portability, but also how to govern data that may be outside of HIPAA's very narrow scope.

But regardless of the regulatory silo, what our members hear from consumers is loud and clear. They want access to their information -- health, education, and financial -- in digital form, and they want to manage it on their smartphone. Moreover, they want all of that to happen in an environment that meets their expectations around privacy and security. This is a tall order, but one that is made more difficult by the lack of Federal privacy legislation, the current odd silos of privacy regulation that put parts of their personal data under HIPAA, others under FERPA, some under GLB.

And what consumers feel like as a random mishmash really devalues the trust that we need in the system. And consumers need to trust our members are delivering the next wave of digital tools and services in a manner that protects privacy and secures data against bad actors. With this in mind, I want to focus on three concepts.

First, expanding HIPAA is a non-starter. HIPAA is a portability and interoperability regime. It is right there in the name. The P stands for portability, not privacy. It is designed for insurers and providers as part of a narrow set of covered entities providing health care services to patients. Expanding HIPAA to all entities processing data with any connection to health like grocery stores under the concept of social determinants of health, would turn the Office of Civil Rights into a second FTC.

Practically speaking, consumers don't need another FTC, especially when the staff of 72 that already oversees 6,000 annual complaints, many of them unrelated to privacy. And we also don't need grocery stores, mapping apps, and smart ag platforms to make all of their data interoperable with electronic health records, which is HIPAA's primary purpose.

But we can't shrug and walk away. Instances where digital health apps process or transfer sensitive personal data in ways that go against consumers' expectations are numerous. After the FTC entered a consent order with period trapping -- tracking app Flo, we sent a letter to this committee arguing that the conduct of Flo is one of the most important reasons for a comprehensive privacy bill. But that privacy bill cannot be an outgrowth of a health record portability law. We need your bill to become law.

Number two, financial services go beyond Gramm-Leach-Bliley, and we need a risk-based framework to better empower consumers. Like HIPAA, GLBA only applies to a narrow, already-defined group of entities. We need to, A, ensure that after financial data is passed from a GLBA-covered entity to the consumer, it is treated as sensitive PII; and B, provide a risk-based framework so that the financial services industry understands where their liability risks are and, most importantly, aren't, so that the industry can spur innovation.

Lastly, FERPA overlaps with the FTC Act and its child requirements under COPPA, resulting in uncertainty for parents, commercial industries, and the education institutions alike. We need to improve clarity and avoid making confusion worse. Some data is opt-out under FERPA, but opt-in under COPPA. This helps no one.

We need to focus on ensuring that a Federal bill benefits all persons of any age, and avoids convoluted fictions like adding a constructive knowledge threshold to COPPA, which will neither be constructive or add knowledge. And we need to modernize verifiable parental consent requirements currently in place so that parents and developers can actually make VPC work, and make it harder for some to simply pretend that all of their audience is over 13.

Ultimately, privacy enforcers need better tools. When Tom Hanks's character was stranded on a remote island in the movie Castaway, he used an ice skate to remove a tooth. What the FTC needs is not more ice skates, tools that don't fit the job and cause more pain than is necessary. The FTC and my members need a statute that specifically prohibits privacy harms resulting from processing, collection, and transfer that go against consumer expectations.

Thank you for inviting me to this important discussion, and I look forward to your questions.

[The prepared statement of Mr. Reed follows:]

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

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

*Mr. Bilirakis. Thank you. Thank you very much.

Our next witness is Donald Codling, senior advisor for cybersecurity and privacy for REGO, the REGO Payment Architectures.

You are recognized, sir, for five minutes.

STATEMENT OF DONALD CODLING

*Mr. Codling. Commerce Committee Chair McRodgers (sic), Ranking Member Pallone, Subcommittee Chair Bilirakis, and Ranking Member Schakowsky, and members of the subcommittee, thank you for inviting me to testify. My name is Donald Codling, and I am the senior advisor for cybersecurity and privacy.

For over 23 years, I worked in the FBI in various investigative programs focusing on international cyber crime and national cyber security operations. These programs particularly emphasize cybersecurity challenges that impact the global financial services, energy, and health care industries. I also served as the FBI's chairman of an international cyber crime working group that consisted of the heads of cyber investigative departments of Australia, Canada, New Zealand, the United Kingdom, and the United States. My experience in cybersecurity and the FBI have taught me to identify areas of cyber risk and assess its threats.

What we are now experiencing in the financial industry is the convergence of several trends that, though individually benign, will collectively cause unnecessary harm to our nation's children.

The first trend is the rapid adoption of mobile devices by children under the age of 18. According to Statista, 97 percent of households with children under the age of 8 either have a smartphone or tablet that the children use exclusively.

Secondly, according to a report by MasterCard, the COVID-19 pandemic doubled consumer adoption of cashless payments.

Finally, the purchasing power of the under-18 demographic has significantly increased in recent years. The National Retail Federation reports that children influence 87 percent of a family's purchases, and pre-teens are spending their own money at over twice the volume compared to 10 years ago. Businesses know the enormous potential of the under-18 market. Yet this perfect storm of financial and technology trends is worsened because Federal laws and regulations have not kept up with the advent of a cashless society.

It is true that the Children's Online Privacy Protection

Act of 1998 makes it unlawful for online companies to collect the personal information of children under 13. This is an opt-in process, while the parent must actively engage and agree to that data collection.

However, most fintech companies that provide financial services products to children adhere to the privacy protections of the Gramm-Leach-Bliley Act of 1999. Under GLBA, companies must offer an opt-out option for non-affiliate data sharing.

But there is no opt-out option for affiliate sharing. This means the default setting for these websites and financial apps allows for the collecting and sharing of data between the ages of 13 and 17 for children with non-affiliated third parties, unless the parent proactively opts out. In fact, there is often no ability for the parents to opt out of sharing of their children's financial transactions between affiliated companies.

Keep in mind that, according to a report by Superawesome, a London-based child privacy firm, by the age of 13 mobile applications have collected over 72 million data points from just one child.

Though Federal laws are currently not adequate to make it unlawful for such behavior, it must be the responsibility of companies to take steps to protect our children's privacy. I am proud to be an advisor for REGO, who has developed the only certified COPPA and third-party GDPR-compliant financial platform for families and children of all ages. REGO is designed to be implemented as a white label offering for banks and credit unions, giving them the ability to provide a secure family banking platform that is fully integrated with their bank's brands and systems.

Since its inception in 2008, the core of REGO was built around the concept of data minimization, where the only information collected for children under 17 is the date of birth. That is it. REGO has created a family digital wallet experience that cannot function without the explicit consent and approval of the parent. This includes requiring parental approval for others to deposit money into the child's account or restricting children to purchase items only from parental-approved vendors: critical security features that many popular mobile payment apps do not have, but should.

In my experience, no other financial technology company has child data and privacy protections so integrated into its foundational strategy except REGO. On behalf of REGO, we support the enactment of strong, comprehensive, and bipartisan Federal privacy legislation like ADPPA that includes strong data minimization, and the data security standards, and will update privacy laws to protect children. We believe that REGO is a perfect example of how you can create innovative fintech products and services that incorporate ADPPA standards, and treat your users as customers instead of as products.

Thank you very much for giving us the opportunity to participate today. I look forward to your questions. Thank you.

[The prepared statement of Mr. Codling follows:]

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

*Mr. Bilirakis. Thank you. Next we have a witness, Edward Britan, from the head of global privacy for Salesforce.

You are recognized, sir, for five minutes.

STATEMENT OF EDWARD BRITAN

*Mr. Britan. Thank you. Chairman Bilirakis, Ranking Member Schakowsky, and members of the subcommittee, my name is Ed Britan. I lead Salesforce's global privacy team, a team of professionals located across the U.S., Europe, and Asia Pacific regions. Thank you for this opportunity to testify. It is a privilege to be here today.

I am passionate about privacy and the urgent need for a comprehensive U.S. Federal privacy law. I have spent almost two decades focused on helping companies comply with global privacy and data protection laws, including roughly two years at Salesforce, seven years at Microsoft, and seven years helping a range of companies at Alston and Bird.

Global privacy laws have changed significantly during my career, with a particular inflection point being effectuation of the EU General Data Protection Regulation, GDPR, in May of 2018. Since then, comprehensive privacy laws frequently modeled on GDPR have passed all over the world. The U.S. is now one of the few developed nations lacking a comprehensive privacy law. The UK, Japan, Brazil, Kenya, and Thailand have all passed comprehensive privacy laws since the GDPR went into effect.

This is not to say that the U.S. has never been a thought leader in this space. In fact, the core concepts in GDPR and most other global privacy laws build upon ideas first introduced in 1973 in a report published by the Department of Health, Education, and Welfare, the HEW Report.

The HEW Report introduced rights to access, delete, and correct personal information; the data minimization inaccuracy principles; and restrictions on automated decision-making. Further, it called for these concepts to be included in comprehensive Federal privacy legislation. Had the U.S. taken that action, our industry, a crucial driver of global innovation and economic growth, might not be facing the current crisis of trust that led our CEO, Marc Benioff, to call for a comprehensive Federal privacy law beginning in 2018.

But it is not too late for Congress to act. The world has advanced the concepts that the U.S. first introduced. Now, as we approach the 15th anniversary of the HEW Report, the U.S. can reassert its leadership by passing a comprehensive Federal law that builds on the current global standard and advances global privacy law for the next 50 years and beyond.

So why do we need a comprehensive Federal privacy law, and what should that law look like?

We need a Federal privacy law because privacy is a fundamental human right. It is also essential for preserving other human rights, such as life, liberty, speech, and freedom from discrimination. Polls show that a majority of Americans, regardless of political affiliation, strongly favor increased legal protections governing companies' use of personal information.

The right to privacy cannot be sufficiently protected by the current sectoral approach at the Federal level or by the individual state laws. The current U.S. sectoral laws are effective and influential, but they are not sufficient. Without comprehensive legislation, there are significant gaps in protection. For example, the Health Insurance Portability and Accountability Act, HIPAA, effectively protects data related to health conditions and provision of health care held -- data held by providers and health plans. HIPAA fails, however, to cover health-related data that may be collected by non-covered entities such as through connected devices and online services that monitor and improve health and fitness.

States have sought to fill the national gap in privacy protection by passing comprehensive privacy laws of their own. Salesforce welcomes this development. These state-led efforts, which have taken place in red states and blue states, are important and demonstrate the need and demand for comprehensive privacy law.

However, one's level of privacy should not depend on their zip code. Congress should be inspired to build upon these state-led efforts in setting a national standard which ensures that these privacy protections are held by all Americans. That Federal law should address core privacy principles, including transparency, individual control, data minimization, security, individual rights of access, correction and deletion, risk management, and accountability.

More specifically, the Federal law should include enhanced protections for sensitive data, children's data, mandatory data impact, and algorithmic assessments, prohibitions on using personal information to discriminate, the controller processor distinction, and restrictions on third-party targeted advertising.

Congress has made great strides toward passing a comprehensive Federal privacy law. Last year this committee passed the American Data Privacy Protection Act, ADPPA, by a resoundingly bipartisan vote of 53 to 2. While there are undoubtedly aspects of ADPPA that every stakeholder would like to change, ADPPA reflected a hard-fought compromise that would meaningfully protect privacy, increase trust in industry, and position the U.S. as a world leader on tech issues.

Salesforce welcomes the role of regulators in shaping responsible innovation. Presently, the world is looking to EU regulators and GDPR to write the rules of the road for emerging technologies like generative AI. With ADPPA, the U.S. has proposed important ideas that should be part of the global conversation.

The path to providing world-leading privacy protections for all Americans is clear. Now is the time for Congress to pass a comprehensive privacy law that builds upon the existing global standard and reasserts U.S. leadership on privacy and data protection. Thank you.

[The prepared statement of Mr. Britan follows:]

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

*Mr. Bilirakis. And last but not least, certainly not least, Amelia Vance from the founder and President of the Public Interest Privacy Center.

You are recognized for five minutes. Thank you.

STATEMENT OF AMELIA VANCE

*Ms. Vance. Chair Bilirakis, Ranking Member Schakowsky, Chair McMorris Rodgers, Ranking Member Pallone, and members of the subcommittee, thank you for inviting me to testify on the need for better child and student privacy protections.

My name is Amelia Vance, and I am president of the Public Interest Privacy Center, chief counsel of the Student and Child Privacy Center at AASA, the School Superintendents Association, and an adjunct professor teaching privacy law at William and Mary Law School. For the last decade I have focused exclusively in my career on child and student privacy.

Children require exceptional privacy protections. They are not yet equipped to weigh the potential benefits and risks of data collection and use. Gaps in Federal laws and a patchwork of state laws mean privacy protections for kids and students are outdated and confusing. Even when clear, these protections contain numerous loopholes that leave children unprotected from companies, predators, and other threats that endanger their health, support systems, and social development, and future opportunities.

Congress should enact baseline Federal privacy protections for all consumers that include additional protections for children and students that recognize children's unique vulnerabilities. Without proper privacy safeguards, children's lives and futures could be irreparably harmed.

I would like to focus my testimony today on a few key points: first, existing Federal law does not adequately protect children and students online; second, efforts by states has -- have primarily created confusion and hampered efforts by schools, districts, and parents to protect kids online; and third, baseline consumer privacy law with special protections for children would be a meaningful step forward to protect kids online.

As discussed in the opening statements, two major Federal laws provide the bulk of privacy protections for children and students online: the Children's Online Privacy Protection Act, COPPA; and the Family Educational Rights and Privacy Act, FERPA. However, both of these have significant gaps that fail to provide children and students with the protections they deserve.

For instance, COPPA only applies when apps or websites collect data directly from children under 13. It does not protect children when websites or data brokers collect information about them. Even more concerning, most of COPPA's limited protections can be easily waived by one click of parental consent.

FERPA only directly regulates schools, not EdTech companies, saddling schools and educators with the burden of policing large companies and corporate data practices. This is an enormous problem, especially since those school vendors are responsible for more than half of student data breaches.

FERPA also only protects student information when EdTech is used in the classroom. The minute that a child goes home and stops using that app for homework, or the teacher suggesting it, FERPA protections go away and companies have free rein.

These are serious shortcomings in Federal law created in large part by lightning-fast growth in tech. Recognizing some of these issues, states have introduced and passed child, teen, and student privacy protections at an astounding rate. But even when these laws have been successful and have not created confusion, we are still left with a legal landscape riddled with far more gaps than many people realize. We need updated Federal data privacy protections.

ADPPA is a strong and important step forward. But when addressing general consumer privacy protections, it is critical to remember children are uniquely vulnerable to certain harms, and we must create meaningful protections to safeguard them. We have all seen recent headlines of dire consequences of insufficient privacy protections. For example, student information including detailed mental health and sexual assault records was posted online after a Minneapolis school district was hacked. The lives of these students are forever changed, and the worst moment of their lives may follow them every time someone Googles their name.

While increasing data security is one method, new protections must also minimize the data that is collected in the first place, and ensure data is deleted when it is no longer necessary. Action to address these harms must be balanced with the real benefits that technology can provide to children learning and social connection. However, we need to make sure that those protections are rooted in a strong underlying, comprehensive consumer privacy law so children are still protected the day after they turn 13 and the day after they turn 18. Thank you so much.

[The prepared statement of Ms. Vance follows:]

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

*Mr. Bilirakis. Thank you so very much, and excellent testimony by all of you. We appreciate it so much.

I will begin the questioning. I recognize myself for five minutes.

In the 1990s Congress responded to the rapid growth of online marketing tactics that targeted children by passing the Children's Online Protection Act mentioned many times, COPPA. In the decades since COPPA's enactment, unfortunately, we have seen far too many violation settlements between the FTC and Big Tech. Instead of protecting children under COPPA's guardrails, Big Tech has determined the value of exploiting kids' data is higher than the cost of FTC fines. In fact, they seem to operate their budgets to account for these fines. This is an unacceptable business practice, I think you all agree.

So this question is for the entire panel, but please be brief in your questions, because I only have a limited amount of time -- in answering the questions. In your experience, what are the ways in which COPPA does not go far enough in its protection of children?

And what are some circumstances where a parent might expect their child's data to be covered, but in reality it is not? Could you provide us with some concrete examples?

We will start from here, sir. Mr. Codling, please.

*Mr. Codling. Thank you, sir.

REGO protects the child's financial data, whether online or purchasing in a retail store, as an example. And part of its basic foundation is data minimization constantly, continuously. And quite frankly, sometimes that hasn't been super popular with the marketing folks. But the mantra has always been do not collect more than the absolute necessary amount of data on that child in particular. Therefore, you don't have to protect something that you have never collected.

*Mr. Bilirakis. Very good.

Ms. Vance, please.

*Ms. Vance. As I mentioned, COPPA is limited to information collected from children, which I think many parents would be surprised by.

But there is also confusion about whether COPPA protects information when you have a label of family-friendly or kid-safe. And many parents assume that, when they download an app or have their child access a website with those labels, it is protected not only from an appropriateness standard, but also from a privacy standard. And it, generally, is not.

*Mr. Bilirakis. Yes, sir.

*Mr. Britan. I think the greatest shortcoming with COPPA, as has already been mentioned, is that it only protects children of 13. Children 13 to 18 aren't protected under COPPA. It is also really hard to identify children. So the best way to protect children broadly is to pass baseline comprehensive privacy law that broadly regulates personal data of everyone, including children.

*Mr. Bilirakis. I am happy to agree with that, sir.

Mr. Reed, please.

*Mr. Reed. I will make this quick. Pretty much everything everybody else said, but I will say one aspect that has been phenomenally important: verifiable parental consent has to work for parents. Right now we call it the over-the-shoulder test. If the device has to go over the shoulder, come back to the parent, and they have to enter in something, the parent then says, you know what, just go to the general audience app.

So as -- we think your bill is really important because it protects people of all ages. Because when we are building the technology, if you make it too hard for the parent to use, then they won't always use it.

*Mr. Bilirakis. Thank you. Congress needs to do -- to once again respond to the new wave of online marketing tactics that fuel Big Tech's ad-based revenue stream and enact a comprehensive, as I said, Federal data privacy law -- everyone is in agreement on that -- to close these gaps. That is why we are having this hearing.

All Americans, no matter their age, deserve privacy protections, just as you said, sir. It is clear that privacy protections should not end when you turn 13.

So my last question, because I am running out of time, Mr. Codling, it seems like you already -- you are already practicing a data minimization principle, as we included in last year's bill. It seems clear that REGO cannot only comply, but continue to succeed if a comprehensive data privacy law is enacted. Is that accurate?

*Mr. Codling. Yes, sir. That is completely accurate.

*Mr. Bilirakis. Okay. You note in your testimony that

REGO is the only certified COPPA-compliant financial platform for families and children. Can you explain what that certification means, and what you have to do to -- what do you go -- how do you get that certification? How do you go through it?

*Mr. Codling. Yes, sir. It requires a very, very detailed audit where a third party -- in our case, a company called PRIVO -- is granted full access not only to our website, but our internal workings, our internal platform. They run tests of placing data in certain areas of an app, as an example, determine how that data is utilized, where is it stored, how is it processed, and, more importantly, how is it protected.

And that audit goes every single year. You look through any time there is a significant change in the app's performance or the app's features, it is run again through this audit, and we are told, yes, you are in compliance, here are some areas you need to fix.

*Mr. Bilirakis. So it is a valuable tool. How many companies are part of this, the certification program, now?

*Mr. Codling. I do not know that, sir, but we can certainly get you that --

*Mr. Bilirakis. Yes, please get back to me on that.

*Mr. Codling. Yes, sir.

*Mr. Bilirakis. All right. I appreciate it very much. Thank you.

All right. Now I recognize Ms. Schakowsky from the great State of Illinois for your five minutes of questioning.

*Ms. Schakowsky. Thank you so much, and I really appreciate the testimony that we are hearing.

The -- we had a hearing last week that dealt with data brokers who are buying and selling Americans' information. And I would like to focus first on health care information. And Mr. Reed, let me ask you about that. So what kind of sensitive information do health apps have right now?

You know, we talked about what is covered, but what are the kinds of things that people ought to avoid, maybe, giving it a little alert that their health data could be collected?

*Mr. Reed. Well, I think right now you are highlighting the problem by having this hearing and pushing for the Federal bill.

We actually operate under multiple state laws that have different perspectives. California has its own tweak on sensitive health information. The reality is, in many instances, it depends on the platform itself and the product itself. Generally, it is the state laws. And for a lot of our members, they have to abide by GDPR. But, as we -- everybody has pointed out, it should be the United States Government that is also providing that insight.

Right now, too much data that people consider to be sensitive personal health information is available in conditions that I don't think people are aware of.

*Ms. Schakowsky. What kind -- can you describe what kind of an app would it be that people --

*Mr. Reed. Well, I think --

*Ms. Schakowsky. -- should avoid?

*Mr. Reed. -- one of the things that -- the best example I can give is there is a very well-known website that has a portion of it that is COPPA that -- I mean, sorry, that follows HIPAA and is a HIPAA-compliant entity, and another part of the website allows people to report their symptoms, and have discussions about their symptoms, and have a sense of community about it. But the information that they are typing into that website is available to be harvested for providing targeted behavioral advertising.

So I think that people often times are misled by, as you said, heard earlier, by the names of the product in a way that can allow that data to flow to data brokers in a way that doesn't meet their expectations, and that harms the health care industry as well as the mobile app industry.

*Ms. Schakowsky. I want to -- your -- in your testimony -- maybe it is just really naive of me, but it says 97 percent of kids 8 and under. Was that the number?

*Voice. Yes.

*Ms. Schakowsky. Are -- either have a smartphone or a tablet.

*Mr. Reed. They have access to a smartphone or a tablet, right. Especially nowadays, when schools are providing this technology as part of the curricula and the way that students are receiving their curricula.

So as Amelia Vance talked about, this gets very important on this overlay between what you are doing at school -- you take your homework home -- or for a growing community, for home schooling, what happens with that information? Does it meet the parents' expectations?

And I would go back to, for my industry, the key thing we need is trust. And when we don't have trust, nobody will buy our products. So it is important that there is a good Federal comprehensive privacy law that help us better eliminate the bad actors, and so that we are not pushed out and we lose that trust.

*Ms. Schakowsky. I wanted to go to Ms. Vance about this issue, too.

Just -- I mean, of course, when I think about education now, kids, little kids, are online. I wonder if you wanted to add it to that -- add to that, what we need to -- how much more we need to do, and why this is a problem.

*Ms. Vance. Specifically related to data brokers?

*Ms. Schakowsky. About children.

*Ms. Vance. About children in general?

Yes, I mean --

*Ms. Schakowsky. Especially --

*Ms. Vance. I think --

*Ms. Schakowsky. I guess beyond the educational, but that they are on their phones.

*Ms. Vance. Absolutely. So as I think everyone knows by now, your phone is the computer in your pocket that tells everybody where you are, what you are doing, sometimes what you are thinking. And that is, of course, so much more sensitive when you are talking about kids who -- their brains are still developing, they may post things or say things that they immediately regret or shouldn't have shared. And that information is already out there.

And particularly when we are talking about outside of the school context, when we are talking about the information coming from someone over the age of 13, or where there is another gap in COPPA, all of that is fair game for bad actors to take it and use it to market products, to potentially sell it, or otherwise --

*Ms. Schakowsky. Let me ask one final question about kids.

Can we fully protect our kids' privacy if we don't also protect the parents' privacy?

*Ms. Vance. Absolutely, we need to protect parents' privacy. Just think of the last Amazon search you did, and the presents that you may have gotten your kids, or a workbook, or a book about a learning disability. That information is incredibly sensitive, and so parental information needs to be protected, as well.

*Ms. Schakowsky. Thank you.

Thank you. I yield back.

*Mr. Bilirakis. Thank you for that question. It is so true. That is why we need the comprehensive bill, because one goes with the other. And so we are filling the gaps.

All right. Now I recognize the chairwoman from the great State of Washington, my friend, Mrs. Rodgers, for your five minutes.

*The Chair. Thank you, Mr. Chairman. A big thank you to all our witnesses for being here today.

I wanted to continue down this line about how we have these layered laws around privacy. We have the FTC Act, we have FERPA, HIPAA, other sector-specific laws, and kind of what Ms. Schakowsky was getting to, the ranking member. Americans think their data privacy is being protected, and yet there is many examples where it actually is not. And part of our goal with a comprehensive privacy bill is to address the gaps and make sure that people are protected, but also that innovation will thrive.

And, you know, this is our sixth hearing, as others have mentioned. It is also -- it is just -- we continue to feel like we -- you know, I want to make sure -- and I wanted to ask Mr. Reed about this -- we celebrate the small businesses, the entrepreneurs, the innovators, and we want that competition to continue as we enact a national data privacy law.

So would you speak to what we have learned as far as the regulatory framework, and what resources do your members have to navigate not only this emerging patchwork of laws now that we see at the state level -- the sixth state just implemented their own state law -- but also the gaps in the other laws?

*Mr. Reed. Well, absolutely. And look, the reality is that, when you are a small business, trust is the most important thing that you can sell. Yes, your product has to work. Yes, it has to be a change element for the company or person who is buying it. But ultimately, nobody is going to use it if they don't trust you. And if you don't have the money to buy a Super Bowl ad, then you need to have an environment where trust is assumed. Therefore, having comprehensive privacy laws help.

And you talked about the state bills that have passed, but I don't know if you realize this. There are 289 currently-introduced state privacy bills happening right now. I have a member of staff, my staff, who literally builds a state map of all of the privacy bills and how they are changing right now. We are happy to provide it for you.

The reality of that is that most of our members -- and this is something super-interesting from an entrepreneurship perspective -- my smallest member, including the ones in your district, are actually international businesses. They might only be 2 people, but they are selling mobile applications in 100 countries around the world. So having a bill that you pass mesh with GDPR is crucial for them to be able to innovate and sell globally, while making domestically.

So from a tools perspective, I hope our trade association can help. That is my job, is to help them navigate it. But what you can do is provide them clear rules of the road that apply to the large companies that provide the infrastructure that we depend on, whether it is the platforms, whether it is the edge providers, whether it is our cloud computing services. If everyone in the food chain has the same set of rules, then small businesses can follow the rules in a way that gets them there.

*The Chair. Thank you. I also wanted to ask you -- because in your testimony you caution us on deferring entirely to the agency rules -- Health and Human Services, HIPAA. As you know, FTC just announced their commercial surveillance rulemaking. It just -- well, it was just weeks after we actually passed our bill out of committee last July.

But would you speak to your concerns around the FTC going its own way to establish rules in this space?

And do you think the FTC by itself has the ability to fill all the gaps created by these current --

*Mr. Reed. Well, the answer to your final -- the last part of the question is no. And we just touched on it with the 289 state bills. The Federal Trade Commission can't issue the kind of preemption that we are absolutely going to need for small businesses to be able to manage their compliance.

*The Chair. Okay.

*Mr. Reed. We don't have 100-person compliance departments in order to do that.

*The Chair. Okay, thank you.

*Mr. Reed. So right off the bat, we can't do it.

*The Chair. Thank you. I want to get to Mr. Britan, too. I wanted to get to some of the new AI models that are -- we see. We see reports every day about companies that are using AI, and there is -- you know, and using reckless, transparent methods when they are incorporating AI into their products.

Just -- would you speak to how risky some of the AI use is in processing of the data, in the heightened risk, and just how a data privacy law might help these new applications for AI? In 30 seconds, yes.

*Mr. Britan. Absolutely, yes. There is no doubt that AI is powered by data, so the best way to ensure that AI is built responsibly is comprehensive regulation of data. And that is how the EU is presently looking at AI, and regulating AI, and examining generative AIs through the GDPR.

And so advancements in AI hold great promise, but they also highlight the need for a Federal comprehensive privacy law, so that the U.S. has a voice in how these technologies develop responsibly.

*The Chair. I appreciate that. We will dig into that more.

Thank you, Mr. Chairman. I yield back.

*Mr. Bilirakis. Thank you. And now I will recognize Ms. Blunt Rochester for her five minutes of questioning.

Ms. Kelly, I didn't see Ms. Kelly. Ms. Kelly, I will recognize you for your five minutes of questioning.

*Ms. Kelly. Thank you, Chair Bilirakis and Ranking Member Schakowsky, for holding this important hearing this afternoon. It is critical that this subcommittee continues the discussions to ensure our nation's laws provide adequate protections for Americans' personal information. So I want to thank the four witnesses for sharing your expertise.

As a chair of the CBC Health Braintrust, I am deeply concerned that sector-specific health care privacy law does not cover vast amounts of consumers' health-related data. Although many think their personal health data is secure, the reality is that consumers have few protections under the Health Insurance Portability and Accountability Act.

In fact, HIPAA does not provide privacy protections for health information, and only limits health data using and sharing by health care providers, health care clearinghouses, and health plans. This allows many health apps, websites, and devices to share information with a host of advertising companies and other uncovered entities. Reports confirm that some of this data transfers include terms like HIV, diabetes, and pregnancy.

Common sense tells us that highly personal, intimate health information should be protected, regardless of the context in which that data is collected and used. Mr. Reed, I have a couple of yes-or-no questions for you. Does information about cardiovascular health become any less sensitive when collected by a fitness tracker, rather than a cardiologist?

*Mr. Reed. No.

*Ms. Kelly. Does information about a patient's symptoms become any less sensitive when collected by a website, rather than a physician?

*Mr. Reed. No.

*Ms. Kelly. Does information about reproductive health become any less sensitive when collected by an app, rather than a gynecologist?

*Mr. Reed. No.

*Ms. Kelly. Thank you for those quick responses. Lastly, Mr. Reed, is there any good reason why apps, websites, and fitness trackers shouldn't be required to safeguard consumers' sensitive health information and treat it with the same care as a physician? And please feel free to explain.

*Mr. Reed. This is the hard part. The legislation you are all proposing has important factors like data minimization and the right to delete. But when something is in your electronic health record and you are a physician, that information, it is really important that it not be deleted, and the physician have the full totality of your record.

So we have to be very careful when we consider who the audience is for the product. A physician that doesn't know about your hypertension because you have deleted it might give you the wrong medication. So when we talk about it in that way, we have to look at it as what does the physician need to know to treat you? And that is critical.

Separately from that, we also want fulsome data so that patients can treat themselves. By 2030 we will be 90,000 physicians short, and communities of color are more affected by that than anywhere else. At the same time, you see tools that allow the management of obesity and type 2 diabetes being absolutely critical to those communities.

So what we need -- and your legislation helps to provide, the committee's legislation helps to provide -- are some rules of the road for sensitive personal information. But I want to be careful that we don't suggest that what the doctor gets is covered in the same way, because the physician must know about your condition over time to properly treat you.

*Ms. Kelly. Thank you for your response.

I also think it is important that any Federal privacy law we consider must strive to end data-driven discrimination. Simply put, any legislative proposal must strengthen civil rights protections by prohibiting discrimination using personal information. That is why last Congress I was proud to support the American Data Privacy and Protection Act, which prohibited covered entities and their service providers from collecting, processing, or transferring data in any way that discriminates or otherwise makes unavailable the equal enjoyment of any goods or services on the basis of race, color, religion, national origin, sex, or disability.

Mr. Britan, how would enhanced protections for specific types of sensitive data, notably data related to race, color, religion, national origin, sex, or disability promote equality and civil rights?

*Mr. Britan. Absolutely. We support those provisions of ADPPA, as well. And those types of protections will give individuals more power to control these sensitive categories of data and how they are used by companies. And I think giving individuals that power is what privacy law should be and data protection law should be all about, adjusting that power balance and giving power to people.

We also support the civil rights provisions that you mentioned that were included in the ADPPA around prohibiting discriminatory uses of data. That is a very important means to protect individuals, regardless of any actions they may take on their own behalf to protect their data.

*Ms. Kelly. Thank you so much.

And again, thank you to all the witnesses, and I yield back.

*Mr. Bilirakis. Thank you. I appreciate it very much, and I will -- five minutes to Dr. Bucshon.

You are recognized for your five minutes of questioning.

*Mr. Bucshon. Thank you, Chair Bilirakis, for calling today's hearing.

Before coming to Congress I was president of a medical practice, I was a surgeon in southern Indiana, and was acutely aware of how important it was to protect the health data and personally-identifiable information of our patients, and to comply with the requirements laid out in HIPAA.

As technology has advanced and society is gathering and utilizing ever greater amounts of data, it is very clear there are gaps in health data protections, as we have talked about some in this hearing. This committee needs to be thinking about the best ways to cover these gaps as it considers a national privacy and data security framework.

Interestingly, I was just with Chair Rodgers in Europe, and we met in Brussels with the EU. We did talk about this and about GDPR. And one of the things I want to make sure we avoid is the effect that we can possibly have on small and medium-sized businesses if we do the wrong thing here. So there is a fine line to be drawn.

Mr. Reed, in your testimony you mentioned cases where non-health information can be used to extrapolate health-related information that -- and that putting extra restrictions on such information would limit consumers' access to digital health tools. I understand that concern, and agree that we do not want to limit access to such tools, but I still believe private health information probably deserves greater protection than many other kinds of data. In fact, for the most part, it is the most monetizable data in the world, health information, in many people's estimation. By that I mean people get your data and they can make money with it, as people know.

Would it be feasible to require disclosures from an entity to a consumer if the entity does use or gather data to extrapolate private health information?

*Mr. Reed. So, Doctor, I think that is something that we continually work on. In your district there is a company called Anew that helps with --

*Mr. Bucshon. Yes.

*Mr. Reed. -- farm elements and agriculture. One of the problems we run into there is, as you know, under social determinants of health you could run into what they do, which is agriculture and food being considered health data. So I agree with you.

And you are right, what we -- we calculate that if I get your full health profile, including key information, it is about $7 a person. It is the most valuable information on the black market possible.

*Mr. Bucshon. Yes.

*Mr. Reed. And so, completely right. I do think, though, we have to think about the totality, and that we don't end up with grocery stores and the company in your district that provides agriculture technologies being there. So yes --

*Mr. Bucshon. What --

*Mr. Reed. Absolutely.

*Mr. Bucshon. Yes, what would be the biggest challenges implementing something like that, if we --

*Mr. Reed. Exactly, exactly what we just talked about: How do we make sure that it is sensitive information about you?

We look at things like physiologic data. Does it record physiologic data about you? We already have that. The FDA already explores these questions of collection of physiologic data. I think those are elements of it. But as you know, we have to preserve the ability to do research, as well. And whether it is through an IRB or other methodologies, we need to be very careful about not requiring such extreme data minimization that you can't do the research we need to do.

*Mr. Bucshon. Sure, I understand.

*Mr. Reed. Or cancer clusters, et cetera.

*Mr. Bucshon. And most research is de-identified information --

*Mr. Reed. Correct.

*Mr. Bucshon. -- anyway, right?

*Mr. Reed. Right. Well, you have to be very careful because, depending on which lawyer you talk to, the definition of de-identified is a moving line.

*Mr. Bucshon. I understand frequently you can extrapolate who it is, based on that.

Mr. Britan, you had comments on that, the same issue?

*Mr. Britan. I would say the same thing, you know, and I would just say be on notice -- notifying people of when that information is being used. We need a regime that protects the data -- that protects data use for these purposes, regardless of whether an individual takes action to protect themselves and providing all these notices --

*Mr. Bucshon. Agreed.

*Mr. Britan. -- it has to be actionable, and I think people should be protected, regardless of whether they take action.

*Mr. Bucshon. Agreed. In fact, I would say the vast majority of people don't know that their health information is very, very valuable, and that it is one of the things that is at biggest risk of all of their privacy data. I am focusing on health here because I was a doctor.

Mr. Reed, are there any guardrails for the use or transmission of personal health information not covered by HIPAA that could protect users in these cases without limiting access to digital health tools?

So what can we -- what should we do?

*Mr. Reed. So I think we are going to be a broken record on this entire panel. I think that we need to move forward with the bill that you have. There are some sections, section 702 -- I mean, sorry, 207 -- where there are elements that could affect doctors like you in terms of having to kind of double dip and be covered by both in a way that I don't think is helpful. But overall, I think comprehensive privacy reform that -- as this panel has discussed, provides notice, provides actionable items, gives tools to the FTC when it is outside the domain of health care is the way to move.

*Mr. Bucshon. Okay. As I said, the -- even some of the EU people who we talk to, they didn't directly admit it, but you could tell by their comments that they do have the concerns with GDPR because of startups, small and large businesses -- small and medium-sized businesses struggling to comply. And we want to avoid that situation here in the United States.

With that, I yield back.

*Mr. Bilirakis. Thank you, Doctor. I now recognize Ms.

Blunt Rochester for her five minutes of questioning.

*Ms. Blunt Rochester. Thank you, Mr. Chairman, and thank you so much to the witnesses. Your testimony makes it abundantly clear that a comprehensive Federal data privacy law is desperately needed in this country.

Last year I was proud to support and vote out of committee the American Data Privacy and Protection Act, and I am ready to work with my colleagues on both sides of the aisle to get this bill passed and to the President's desk for signature.

While there are several gaps in our current sectoral privacy regulation system, I am alarmed by the rise of dark patterns, especially for children, and the use of health data without effective regulation. Over the last several years the FTC has detailed the ubiquity of dark patterns that misled consumers, as well as the misuse of health data on apps not covered by HIPAA.

To follow up on Ms. Schakowsky's questions, Ms. Vance, your testimony highlights the issues surrounding manipulative device design practices, often known as dark patterns, that are intended to trick people, including children, into making ill-informed choices. While deception isn't a new problem, deception and manipulation in the age of social media and mobile apps has changed the game. That is why I am planning to reintroduce the DETOUR Act, which would crack down on deceptive design practices that undermine user autonomy.

Ms. Vance, in your opinion, how pervasive a problem are dark patterns?

*Ms. Vance. I think we see across the Internet that they are everywhere. Every, you know, smaller "no, I don't want this'' button, every "no, I don't want to be smart when I don't subscribe to this newsletter,'' and sort of pushing people to stay on, and keep on the apps and the games and the website, which is maybe good in the case of a math app and getting kids to read more, but incredibly problematic in manipulating people against their will with no idea that it is happening.

*Ms. Blunt Rochester. Yes. I have to tell you, I -- for a while there I thought it was me, but I literally could not find these little Xs to X out of things. I mean, I know I am not the only one now, and it is just ridiculous.

And, you know, are dark patterns especially pernicious when it comes to children's usage of online products?

*Ms. Vance. Absolutely. Children's brains are still developing, and they won't necessarily notice as easily as an adult might that they are being pushed in a certain direction, or driven further down a rabbit hole of videos they are watching, or monetization from games.

*Ms. Blunt Rochester. Yes. Well, given the examples that you noted in your testimony, do you believe a comprehensive privacy bill that includes regulations on dark patterns is a more effective approach than a privacy bill that only protects children?

*Ms. Vance. Absolutely, especially since those, when they turn 18, go to higher ed, and that affects all of their futures.

*Ms. Blunt Rochester. Yes.

*Ms. Vance. It is essential.

*Ms. Blunt Rochester. Thank you.

And any other -- Mr. Reed, I see you have got your hand up -- on dark patterns?

*Mr. Reed. I think it is important to note that the issues you are talking about, about not being able to find the X, that actually hurts small businesses a lot.

If I have a mobile app, the numbers are very simple. If I build an application and I charge $1 for it on the store, I get 1 download for every 100 I get of an ad-supported application. But if you download my ad-supported application where I am using someone else to provide that ad, and you can't find the X, you stop using my app.

*Ms. Blunt Rochester. So true.

*Mr. Reed. So the issue, as she points out, I don't care how developed your brain is, if you can't find that X, you stop using my product.

*Ms. Blunt Rochester. Right.

*Mr. Reed. And so, as we clean up the industry, as we have this kind of legislation, it helps everyone do a better job.

*Ms. Blunt Rochester. Yes, yes.

*Mr. Reed. Thanks.

*Ms. Blunt Rochester. Thank you, Mr. Reed.

Mr. Britan, did you have something you wanted to share on dark patterns?

*Mr. Britan. Sure, yes. I would just say Salesforce strongly believes that people should not be misled or tricked into making decisions based on dark patterns. I think the DETOUR Act would help in this regard, and the DETOUR Act as part of a comprehensive bill would be even better.

*Ms. Blunt Rochester. Thank you so much.

And Mr. Codling, is there anything you want to share on dark patterns?

*Mr. Codling. Not directly with dark patterns, but as an example, because REGO is COPPA-certified, part of that certification process is to review the privacy policies, to look at the websites, and specifically not allow certain dark pattern kind of behavior to make the privacy policy age appropriate.

So there is one privacy policy for the parent and there is one for the child to say, here is what we are doing with your stuff, and here is what we are not doing with it. It goes to your point, ma'am, about can I find the X quickly? Yes.

*Ms. Blunt Rochester. Yes. Thank you so much. I have some additional questions that I will enter for the record for Mr. Reed, particularly on HIPAA and the health aspect of this, the health -- I am on the Health Subcommittee, as well.

[The information follows:]

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

*Ms. Blunt Rochester. And so I will yield back the -- actually, I don't have time to yield back, but I will yield back the time I don't have. Thank you.

*Mr. Walberg. [Presiding] You always have time. You always have time to yield back.

*Ms. Blunt Rochester. Thank you.

*Mr. Walberg. I thank the gentlelady, and I recognize myself for my five minutes of questioning.

And thanks so much to the panel for being here. This is a topic, as we have said, we must continue looking for solutions.

Children's privacy protections need to be updated. That is very clear. Whether at school or at home, there are significant gaps in how their information is protected. The pandemic and forced school closures made that even more clear. I am glad that there were so many online resources for parents and teachers and grandparents to turn to when their children were unable to go to school. Educational apps and websites offer immense benefits, and I would much rather my grandkids use them over social media. We at least can choose those apps.

But there are also very concerning reports of these apps and tools collecting and selling children's data for advertising. An article by the Washington Post last May reported that nearly 90 percent of educational apps and websites were designed to send the information they collected to advertising tech companies to help them predict potential buying habits of kids. Some EdTech platforms unnecessarily request access to students' cameras and locations.

And so I would ask for unanimous consent to include that article for the record.

Without objection, and I -- hearing none, it will be included.

[The information follows:]

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

*Mr. Walberg. I serve on the Education and Workforce Committee, as well, which has jurisdiction over the Family Educational Rights and Privacy Act, or FERPA. I have also been an avid supporter on this committee for updates to COPPA and kids privacy, overall. With at least a decade behind us since either of these laws were updated, neither of these laws reflect the realities of today's digital world.

Mr. Vance, there are clearly gaps and confusion on when and to what extent -- excuse me, Ms. Vance -- these two laws protect children's privacy. What is the result of this confusion for kids, parents, and schools, and how do we provide greater clarity?

*Ms. Vance. As Morgan was saying, they lose trust in vendors, in their schools, in other parents, in society itself. It undermines everything we do if we can't do the digital equivalent of step outside our front door without some harm potentially falling from the sky.

And so it is incredibly important that we have these comprehensive privacy protections, with heightened protections for children.

*Mr. Walberg. Mr. Reed, as I said, the explosion of digital education services is great, but I am extremely concerned how common and easy it is for apps to collect, store, and sell children's data.

In your testimony you indicated that COPPA and the FTC's guidance sufficiently holds EdTech and schools accountable for their privacy practices. But obviously, significant amounts of information about kids are being collected and sold by these tools every day. Where does the issue lie?

*Mr. Reed. I think, in the case of my testimony, I misspoke in the sense of sufficient, in the sense that they have authority over sufficient areas, but the gaps are huge.

One of the areas that creates the greatest concern -- I think it is really important you talk about -- is verifiable parental consent issues. I appeared before this committee, I think, in 2010 as a vociferous advocate for VPC. Unfortunately, verifiable parental consent has not taken the world by storm. And instead, what you see is even limited amount of friction causes parents to basically say, well, use the general audience portion of the application.

One of our members actually provides -- is a safe harbor, and provides services to another person on this panel. And what they find is the cost of getting the parent engaged and to do these steps is often times something the parent doesn't want to do. As I talked about earlier, we call it the over-the-shoulder problem. The moment the parent can say, oh, go to the kid's YouTube, it is too hard, go to regular YouTube, we have lost them. I testified multiple times at the FTC about this.

We need to have the platforms that are part of our ecosystem have more flexibility to provide either credentialing or flags to my members to say, "Hi. To the best of our knowledge, this user is a child. You need to behave in this manner when we pass that flag.''

Unfortunately, right now you heard my fellow panelists talk about auditing. The platforms are not in a stage where they want to audit 1.5 million applications that are currently on their platforms. But if there were a way for the FTC to be more flexible in providing that flag, then that is something that the FTC, through your authority, can use to say, hey, you were provided this flag, you didn't use it, you didn't get rid of that information. It is a tool the FTC can use to get to what you want.

But merely expecting more from parents is not going to get the solution that you are after and that, frankly, all of your panelists are after.

*Mr. Walberg. Well, clearly, yes, we are -- a comprehensive privacy law would fill many of the gaps we discussed today, but I also believe that we need to take another look at both FERPA and COPPA.

Thank you. My time is ended. I yield back, and now I recognize Representative Clarke.

*Ms. Clarke. Thank you very much, Mr. Chairman, and I thank our ranking member for holding today's hearing.

I would also like to thank our witnesses for being here to testify on such an important issue. Passing legislation to fill the gaps in current privacy laws is long overdue, and I remain committed to working with my colleagues across the aisle to pass a bill that protects all Americans' data.

Mr. Britan, in your testimony you cite the EU's GDPR as a driver of core privacy concepts like data minimization, the right to access, delete, and correct data, and guardrails on automated decision-making. In your opinion, does the U.S.'s lack of a comprehensive national privacy standard inhibit our ability to lead or even participate in the global conversation on rights to data privacy and human rights?

*Mr. Britan. Absolutely. And it is table stakes to enter those conversations. I believe we share these values with our allies all over the world. But at some point we have to demonstrate that through action.

*Ms. Clarke. Absolutely. I see you nodding your head, Mr. Reed. Would you like to add your position on that?

*Mr. Reed. I think Mr. Britan said it as well as any of us can, which is we need to demonstrate through action.

*Ms. Clarke. Very well. Mr. Britan, I would like to follow up and ask how the lack of a clear national standard will impact the U.S.'s ability to lead in data-intensive innovations like generative AI, quantum computing, and smart cities?

*Mr. Britan. Salesforce welcomes regulation, and regulation is really important for ensuring that these new innovative technologies are released in a responsible manner. Because if we release it in a way that reduces trust, it is virtually impossible to regain that trust.

And there is important global conversations happening right now. This is an amazing time for tech innovation, and the U.S. needs to be part of that conversation. In order for the U.S. to be an effective part of that conversation, we need comprehensive privacy law.

*Ms. Clarke. We can't be the weakest link, in other words.

[Pause.]

*Ms. Clarke. Absolutely.

Okay. Mr. -- sorry -- Ms. Vance, do any parts of COPPA require analysis of how algorithms may disproportionately cause harm to certain groups?

For example, some algorithms may show content that may be more dangerous if shown to children than the general population. Is there anything in COPPA requiring companies to look into how their algorithms affect children?

And what about FERPA?

*Ms. Vance. No, there is not in either law. And that is part of the reason why ADPPA was so exciting for me, because that is an invaluable and important protection.

*Ms. Clarke. Very well. Well, it is my position that comprehensive privacy legislation is long overdue and absolutely necessary for the U.S. to maintain leadership in a range of industries driving innovation. Our laws have failed to keep pace with revolutionary innovations, leaving Americans more vulnerable to discriminatory algorithms, invasive data collection, and cyber attacks. Increases in the amount of data available have earned -- have created enormous and unprecedented consumer benefits. But we need legislation to ensure vulnerable populations are not -- are, excuse me, are protected against discrimination, exploitation, and manipulation.

So I want to thank all of you for your expertise and bringing it to bear today in this -- in today's hearing. We look forward to working with you as we move us into the 21st century, as I like to say.

And with that, Mr. Chairman, I yield back.

*Mr. Bilirakis. [Presiding] I appreciate that very much. Now I will recognize Mr. Duncan from the State of South Carolina for five minutes of questioning.

*Mr. Duncan. Thank you, Mr. Chairman, for holding this hearing and the continued work that you are doing on this important issue.

I want to ask all four witnesses -- and I will start with Mr. Britan -- from whom should we be protecting the data of American citizens? Who is the greatest threat here, is it Russian hackers, Communist Chinese, big American companies, identity thefts, predators?

And from your unique perspectives, who is the threat that we, as policy-makers, need most to focus on to protect our citizens, especially kids and teenagers?

*Mr. Britan. Those are all significant threats that I think a comprehensive privacy law would help us to address.

The greatest threat is going to be the one that we don't know about, and it is really hard to predict. And I think baseline protections that include data minimization, and treating data as a potential liability, and the reduction of data, and managing data responsibly and in an organized fashion, understanding who has access to the data, and that sort of data management capabilities is the best way to address all of those threats.

*Mr. Duncan. Okay. Mr. Reed?

*Mr. Reed. I think we have to be thoughtful. All of those are good, but there is a company in your district, Topography Digital, that does drone and a lot of other really cutting-edge technology. I think we have to realize that the biggest threat to the success of the companies in your district, like them, is the unexpected, for the loss of trust that happens.

So when we talk about threats from outside influences, what you really see is most of the data ends up in the hands of somebody who isn't going to do harm, just wants to make money off of it. But that destroys the trust and degrades the value of the systems we are providing.

So on the one hand, you absolutely should be focused on the international threats and the security, but we also need a comprehensive bill so that consumers know what to do and what the products are going to do to them, so they know if they are going to share the data. So it is the insidious ones that aren't there to harm, just there to make money off of it, that create the loss of trust sometimes.

*Mr. Duncan. Yes.

Ms. Vance?

*Ms. Vance. I can't agree enough with my fellow panelists.

I would add anything that has the opportunity to destroy a child's future, whether it be information that data brokers are collecting and sharing with anyone who asks for it, or the use of that information by stalkers, parents with restraining orders, pedophiles, et cetera, that is really, I think, the greatest threat.

*Mr. Duncan. Mr. Codling?

*Mr. Codling. Your question is excellent, sir, so I will split it into two areas. There is the criminal activity and then there is the national security activity.

Criminal activity, cyber crime organizations, have become truly globalized. They have vertically integrated their capabilities to the state that they are as good as nation states, some of these criminal activities.

A national security standpoint, of course, you have got to be very concerned about the Chinese, Russians, Iranians, North Korea.

But a perfect example from a child's privacy protection standpoint, the worst case scenario is something like TikTok or some other social media platform that can come in, aggregate the data that the child in this case is utilizing from the social media standpoint, and if that company platform also offered financial services capabilities, because those are affiliated companies that data is going to flow back and forth between those two. And Lord only knows where that stuff will end up.

So in my FBI career we spent a lot of time finding out where that stuff ended up.

*Mr. Duncan. Yes.

*Mr. Codling. Typically, it was not in your home district. It was overseas someplace.

So just last week, TikTok made an announcement that they are very interested in working with large American retailers to allow individuals on the TikTok platform to purchase, buy, engage in commerce. To me, as an uncle, that is a nightmare. There is no good end of that with that particular company. I am not going to paint everybody in the same way.

It does scare me, because I can now build a complete data dossier on that individual as a young person, and have now those last couple of little gaps filled in. I know who you are, and what you are, and what you have been doing since -- pick an age. That is very, very concerning.

*Mr. Duncan. Yes. Okay. If Congress were to pass a Federal privacy law, what single provision would be the most essential factor in that new law being successful?

And I will ask Mr. Codling.

*Mr. Codling. I think having a comprehensive law, sir, puts the United States, to my -- the panelists' opinion -- back in the game. We should be the leaders. We were the leaders.

*Mr. Duncan. Yes.

*Mr. Codling. We can be again.

*Mr. Duncan. Let me ask Mr. Britan real quick. Mr. Britan, same question, yes. Eight seconds.

*Mr. Britan. Yes, I think the key is to build these responsibilities and apply these responsibilities to the companies that process data, and ensure they are processing it responsibly.

I think the notice-and-choice regime has failed. It puts too much burden on the individual. We need a comprehensive law that comprehensively regulates data.

*Mr. Duncan. Yes, identify the threat --

*Mr. Reed. I am going to say one word: preemption.

*Mr. Duncan. Yes, yes, oh, yes. Identify the threat and then craft something to combat it. And you do that in football, you do that in war.

So I yield back.

*Mr. Bilirakis. I thank the gentleman, and I will recognize Ms. Castor from the great State of Florida, and my fellow Tampa Bay resident. Go Rays.

*Ms. Castor. Go Rays. All right. Thank you, Mr. Chairman, and thank you to all of our witnesses for being here to discuss data privacy.

I strongly support this committee moving forward expeditiously with a comprehensive data privacy law that protects the personal privacy of all Americans, and I have been particularly focused on the harms to children, and just recently filed -- re-filed my Kids PRIVACY Act that was developed with advocates like you, and parents, and pediatricians from all across the country. And it is time to act. I was heartened last session that the committee included portions of the Kids PRIVACY Act in ADPPA, but we really need to move forward quickly.

And on kids, one of the things that we aim to do is raise the age. Right now there is -- really, it is just kids 12 and under who are protected. Ms. Vance, is there any reason that we shouldn't give all adolescents a fighting chance here, and protect their privacy by increasing the age?

*Ms. Vance. I think that is absolutely vital.

We also need to recognize, though, that teenagers have different needs, are at a different developmental stage. And so making sure we are taking that into account, as well, is really important.

*Ms. Castor. That is why, in the Kids PRIVACY Act, I created a protected class, so it is not quite as stringent as COPPA, but the Children's Online Privacy Protection law right now, it is so outdated. When was it first adopted?

*Ms. Vance. In 1998.

*Ms. Castor. In 1998. Think of all the technological changes since 1998 in this huge surveillance and data-gathering enterprise that exists right now. We have got to move now to update this.

You also, Ms. Vance, in your testimony highlight the fact -- you kind of compare what the Europeans did in the GDPR, which is their privacy law, and then explained in your testimony that they followed on with an age-appropriate design code. So that is actually missing from ADPPA. Do you recommend that the committee also begin to develop an age-appropriate design code? Some states have done this, as well, but -- what is your recommendation?

*Ms. Vance. I think it definitely needs to be based on the foundation of a comprehensive consumer privacy law, and that is really what has led to a lot of the successes in the UK with their age-appropriate design code.

Obviously, the EU legal landscape versus the U.S. legal landscape is not the same. So there is a lot of details to work out, as California is finding out. But the principles, the underlying, you know, location, off-by-default, just-in-time notifications, consideration of different age ranges and what is appropriate, all of that are protections that should be here.

*Ms. Castor. Isn't it interesting that some states are moving to banning social media outright? And it is such -- it seems like, you know, it is appealing, it is kind of a -- based upon all the harm that we know that it is causing to mental health, addiction, and things like that.

But wouldn't privacy protections come first, and then a design code to require that apps and platforms actually design their products with kids in mind? Isn't that the most important thing that we can do right now, and is -- I don't know that banning social media is even -- if that is even realistic. What do you think?

*Ms. Vance. I completely agree. We shouldn't punish kids for the bad actors, whether it be the companies, individuals on social media, or websites, or apps. We should acknowledge we need to protect the spaces that they are going to go into.

We all know how innovative kids can be when it comes to getting around particular restrictions. And so it really is important to make the world that they are living in, that they are going to go into safe, no matter what website or what app it is.

*Ms. Castor. And we have the ability and the authority to do that by passing new, modern laws that put the kids' interests first, and direct that apps and platforms actually develop these with kids in mind, and then not allow them to target children with advertising. That is pretty basic in privacy laws that are being adopted across the country towards -- for children, isn't it?

*Ms. Vance. Absolutely. Almost every 1 of the 140 state student privacy and child privacy laws that have passed in the past decade ban targeted advertising across the board for kids.

*Ms. Castor. Well, I encourage the committee to move expeditiously, and I thank the witnesses and Ms. Vance for being here. Thank you.

*Mr. Bilirakis. Thank you. I now recognize Dr. Dunn from the State of Florida for your five minutes of questioning.

*Mr. Dunn. Thank you very much, Mr. Chairman.

At our last hearing I mentioned that the Chinese Communist Party seeks to sabotage freedom and democracy everywhere that it exists. And this mentality permeates throughout all of China's corporations, as well, including those that operate in America.

Despite American leadership and technology, we still do not have a comprehensive national privacy standard. Ironically, China does.

However, China's privacy law, the personal information protection law, is in reality a national surveillance plan. Their law forces data sharing of every person and business in China with their government. Their law puts everyone's personal details at grave risk of government surveillance, and their law enables their government to individually target citizens for concentration camps, enslavement, and even death. It literally enables the Chinese Communist Party to target individuals who are a potential source for organ transplantation, and the government knows whose genetic codes match whose, and they will murder and steal organs at will. Thus, their law does not protect privacy at all. It gives all their data to the government. Most of all, it certainly doesn't keep China from hacking Americans' data.

I want to remind my colleagues and my fellow Americans of some of the largest data breaches in the last decade, all of which left millions, hundreds of millions, of Americans' data exposed.

[Chart]

*Mr. Dunn. I refer you to the poster behind me, starting with Yahoo and going down to the final entry there, U.S. Government employees with security clearances, 20 million hacked.

The American Data Privacy and Protection Act is both a privacy bill and a cyber security bill, and we need both. Protecting Americans from privacy invasion by domestic and foreign companies is important. And when we choose to share our data voluntarily with them, the security of our data in that company is also essential. Information that is not secure cannot be private.

Without a comprehensive privacy standard, we can't stop Big Tech, the Communist Chinese Party, TikTok, or anyone else. When Big Tech and data brokers compile large troves of data, they are creating massive targets for malicious Chinese hackers and others. We cannot allow them to profit from our loss or inattention.

Mr. Britan, thank you for your testimony. You have spent the last two decades working on global privacy and data protection policies. In hindsight, what are the key Federal provisions you would recommend to protect Americans' data?

*Mr. Britan. I think a strong Federal law has to have all the rights that were first introduced in the Hew report that exist in GDPR and most global laws: the rights to access data, obtain a copy of data, to delete your data. I think that the -- but that is not enough. That is the first step.

We couldn't -- we can't -- we shouldn't put the burden of protecting privacy entirely on individuals. I think what really sets ADPPA apart are the obligations it puts on companies to protect individuals, regardless of whether or not they exercise their rights. And those are obligations around mandatory assessments, obligations around corporate responsibility, and the duty -- the duties that are included in ADPPA for companies.

*Mr. Dunn. Excellent, excellent. So there are certain guardrails we think should be put -- we talk about it as minimization of data, but guardrails on what data is being allowed to be collected and by whom. Can you comment on that, Mr. Britan?

*Mr. Britan. Yes, absolutely. I think data minimization is -- we view it as a good thing. It is not a new concept. As I mentioned, it is something that has existed since the Hew Report.

I think the key thing that ADPPA does is it forces data collection to be purposeful. It forces you to think about the data you are collecting, and why you are collecting it, and have a strategy. And as you mentioned, that is going to be so critical for minimizing the data we have, ensuring we have it for the right purposes, ensuring that we have proper access controls around that data. That all has to be documented and analyzed under ADPPA, and that is going to be some of the best protection we have against the threats that you identified.

*Mr. Dunn. Thank you very much.

Mr. Codling, in your testimony you mentioned that your experience with the FBI has informed your conducting cybersecurity assessments. What, in your opinion, is the most vital and vulnerable personal information the government collects on individuals?

*Mr. Codling. I am going to follow some of Mr. Britan's comments of data minimization, data minimization, data minimization, all day long. Then you have less material to defend. You have less material to be concerned about if you never collected it.

Data thieves are completely going to go after children's data, particularly their financial data. And the fact that you have a blank slate when you are a young person, data thieves, nation states can come in and destroy your credit before you even realize that you needed credit.

*Mr. Dunn. Ah, the Equifax hack. Well, thank you very much to the entire panel for your time and testimony.

Mr. Chairman, I yield back.

*Mr. Bilirakis. Thank you very much, Doctor. I will recognize now Mrs. Trahan for her five minutes of questioning.

*Mrs. Trahan. Thank you. Thank you, Chairman Bilirakis and Ranking Member Schakowsky, for calling this important hearing.

Today's meeting is just another example of the bipartisan consensus on this committee that the current laws governing the Internet fail to protect users and our most sensitive information. And it further highlights the importance of passing a strong, comprehensive privacy law like the American Data Privacy and Protection Act, and doing so urgently.

As many of my colleagues on the committee are aware, I am deeply concerned about what the emergence and embrace of education technology means for privacy and data of our children. Students and parents rarely have the option to withhold consent when using education technology or providing their data for platforms and devices used by schools. That is why I unveiled draft legislation two years ago to detail concrete steps Congress should take to protect student privacy and rein in tech companies.

And I am grateful that, when this subcommittee met to consider ADPPA last Congress, the chairman and ranking member worked closely with me to improve the bill to specifically protect students, including an important clarification that EdTech companies are not exempt from the bill simply because they work with schools.

Ms. Vance, in your testimony you mentioned that EdTech companies must comply with FERPA only to the extent that schools negotiate those restrictions in their contracts. In your opinion, do you think it is right to place that burden on schools?

And do you believe they have secured sufficient privacy protections for their students in those negotiations?

*Ms. Vance. It is absolutely unfair to put that burden on schools, just as it is to put child privacy protections burden on parents. You often don't have a dedicated privacy person, security experts, and others who can adequately protect that. And whether a company is small or large, they have more personnel who can do that than an individual school.

*Mrs. Trahan. Well, I couldn't agree more. I don't think superintendents or principals should be responsible for negotiating our kids' data rights with multi-billion-dollar companies. And I certainly don't believe that parents should have to pore over school district contracts with EdTech service providers to understand where the protections negotiated by their schools are strong enough. At the end of the day, the burden should be on the companies to design their services with privacy at the forefront, and minimize the data that they collect.

There is bipartisan agreement that data on minors should be considered sensitive data, but there are different views on how we should set standards for when a company knows a user is a minor. Ms. Vance, again, would you agree that, regardless of the company's size, a company should protect user data as sensitive children's data when the company targets and markets the products to serve K through 12 students?

*Ms. Vance. Absolutely.

*Mrs. Trahan. I agree. And we have discussed three circumstances where companies generally must take extra measures to protect kids data: first, in the school setting, where education records collected -- excuse me, where education records collected by most schools are protected; second, when companies direct services towards children; and third, when companies have actual knowledge that users are children.

Are there other circumstances where you think companies should give heightened protection to kids' data, and can you explain how you think about those requirements?

*Ms. Vance. Absolutely. We briefly mentioned the UK's age-appropriate design code in a previous question. The creator of it asked a question on a working group I was in several years ago: What if kids didn't have to lie to be on the Internet? What if they could have the same experience? And that doesn't mean making the internet kid-proof; it means I can say that I am a kid, I can say that I am a teen, under 18, and have tracking pixels and other things turned off.

*Mrs. Trahan. Yes.

*Ms. Vance. And I think that isn't something that we have necessarily considered here. It doesn't have to be a kid-proofed Internet or a Wild West. It can be a good place for kids to grow up in.

*Mrs. Trahan. Well, I share those concerns and that view of how the Internet could be. And I think that there are important lessons here.

As our committee discusses the failures that exist in other laws, we always need to be on the lookout to strengthen the legislation that we work on and pass today. So I am grateful, certainly to the chairman and ranking member, members of the subcommittee, for their continued attention to these important issues, but really grateful for your expertise and bringing that to the subcommittee today.

I yield back.

*Mr. Bilirakis. The gentlelady yields back. Now I will recognize the gentlelady from the State of Arizona, site of the NFL draft tonight.

I will recognize you for five minutes of questioning.

*Mrs. Lesko. Thank you, Mr. Chair.

Mr. Reed, according to a January 2022 report from the Information Technology and Innovation Foundation, the growing patchwork of state laws will cost small businesses at least $200 billion over the next 10 years. Given the differing levels of size and sophistication that businesses may have, how important is it to small businesses that a data privacy law is clear and consistent throughout all of the 50 states?

*Mr. Reed. It is absolutely essential for all the reasons you outlined. And I think what is most important about what you are trying to do is it is not just the small businesses that will end up complying. It is all of the third parties that we depend on to build our products.

Software is built like Lego. We write something special, but it is built of parts from other things, whether it is a software development kit or any other tools that we need. When everybody has the same rules, it helps the small business build something unique and special out of the pieces that we all see out in the table.

*Mrs. Lesko. Well, and related to that, my next question, follow-up, is if we keep the status quo and the patchwork of state laws continues to grow, how can we expect entrepreneurs to take risks and innovate? Will they?

*Mr. Reed. No. And a very good example during GDPR, which we have kind of all gotten to deal with, one of our members came to me and said, "Well, so for the past year I have had one of my programmers, a full FTE for an entire year, just going back through to make sure we complied with GDPR.'' It is a five-person shop. Now it was -- for a year it was a four-person shop. That means there were jobs they didn't bid on, projects they didn't build, innovations they weren't able to put into it. And if I have to do that for 50 states, hire 50 different people doing a single year's worth of FTE to comply, it is simply unworkable.

*Mrs. Lesko. Yes, I can definitely see that.

The next question is to any of you. Is there a state data privacy law that this committee should look at that is a good example that we should either replicate or use parts of it?

*Mr. Codling. Yes, I will throw out California, because California Consumer Rights Act and California Consumer Privacy Act were leading-edge. They actually said we have a problem, let's tackle it. It may be a fight in the mud puddle, but let's tackle it and let's move the ball forward. So kudos to them. And several other states have followed suit with that.

*Mr. Reed. I am going to go in a different direction. Virginia and five other states -- Virginia, Colorado, Connecticut, and others -- have done bipartisan legislation that I think is worth looking at.

*Mrs. Lesko. All right, very good. One last question, and this is, quite frankly, to any of you.

What changes, if any, should be made to the American Data Privacy Protection Act that we passed out of committee last Congress to make sure we put consumers in control of the data shared through their smart home systems?

*Ms. Vance. I think one of the really important things, as I mentioned, there is a lot of intangible privacy harms when it comes to kids, when it comes to all of us. And so making sure that we are really looking at protecting not only a physical safety issue, but also something that may happen down the road, the misuse of information that we don't know yet is going to happen, but history tells us it almost certainly will. So including more protections against those sorts of intangible harms would be invaluable.

*Mrs. Lesko. Okay. And does anybody have any input on specifically smart home systems?

[No response.]

*Mrs. Lesko. No? All right. Well, thank you.

Oh, Mr. Reed?

*Mr. Reed. Just that a smart home system is, at the end of the day, a way to collect data that should serve the consumer who buys it, right? I get a smart home system because I want to be able to answer questions in my kitchen. I want the Alexa when I say, "Don't forget that I need to buy milk,'' to do it. The question is what is done with that data moving forward.

So I think, when we look at smart home systems, I think, as Ms. Vance said, there is some physical security elements when it locks your door, when it shuts off your lights that are in question. But I think you should look at the totality of it, which is it is collecting data on you that should be used for the purpose that you want it to do, remind you to take out the garbage, play a song, not ship that data to somebody else, to a broker that you didn't expect, that ends up shipping you something that you didn't want.

So for that reason, I think smart homes are sensitive, but it is part of the larger picture of, hey, I am -- I want a service, and this is what you are doing with the data.

*Mrs. Lesko. Thank you. Thank you for all of you coming here and spending hours with us. I appreciate it.

And I yield back.

*Mr. Bilirakis. Well, I tell you what, you asked some great questions, Mrs. Lesko. Thank you very much.

I yield back -- she yields back, and we are going to ask Mrs. Dingell to ask her -- she has five minutes of questioning.

You are recognized.

*Mrs. Dingell. Thank you, Mr. Chairman. And I want you to know the NLF (sic) draft is in Detroit next year.

*Mr. Bilirakis. Next year.

*Mrs. Dingell. The Debbie Caucus is cheering for the

NFL.

But thank you, Mr. Chairman and Ranking Member --

*Mr. Bilirakis. That should be exciting. Am I invited? Am I invited?

*Mrs. Dingell. Well, did she invite you? I will.

*Mr. Bilirakis. I will hold you to that.

*Mrs. Dingell. I will. Anyway, thanks for both you and Ranking Member Schakowsky for holding this important hearing, and this is a subject that is very important to me.

As I have highlighted at several of these hearings focused on privacy, we have got to ensure that consumers are the ultimate arbiter of the data while allowing companies to perform any action that consumers should reasonably expect from the use of a platform device or any other technology. And as we all know, but -- we do, but too many consumers don't -- many platforms are already collecting far more data than most consumers expect or know, and it is much to their detriment.

But we must also take into consideration how gaps in current privacy law have led to vulnerabilities, such as those presented by notice and consent regimes and their impact on consumer and industry behavior that we must ensure are addressed.

Neither a consumer that dutifully reads the terms of service of a platform nor one -- and I think this is most people -- that immediately click yes to this consent request currently have sufficient baseline privacy protections and availability of consumer choice in the current landscape. And I think it is crucial that Congress address this gap in any comprehensive privacy legislation we advance through committee and the Congress.

So notice and consent. To best safeguard America's sensitive information we need privacy by design, not privacy through pop-ups. Unfortunately, our fragmented Federal privacy laws heavily rely on the failed notice and consent regime. As anyone who has ever opened up a checking account or filled out paperwork at a doctor's office or applied for a credit card online can tell you, notice and consent does not actually involve meaningful consent or consumer choice. It is simply impractical, especially online, where consumers may visit dozens of websites in any given day. And quite frankly, they want to get rid of the pop-up. They don't realize how it is impacting their life.

Mr. Britan, do existing privacy laws provide consumers with a meaningful opportunity to understand and say no to an entity's data practices?

*Mr. Britan. Thank you for this question. I 100 percent agree with you that notice and choice has failed as a privacy regime. It puts too much burden on the individual. It is unfair to the individual. There is no -- most individuals don't have the time or the wherewithal or the ability to find all the information they need to make meaningful decisions.

And individuals should be protected, regardless of the decisions they may or may not make. There need to be baseline protections. I think -- that is not to say that notice and choice isn't helpful, and that we should get rid of notice and choice altogether. I think it just should not be the end of the story. And there need to be clear obligations and protections that apply to individuals, regardless of any decisions they may or may not make.

*Mrs. Dingell. Thank you. I believe that we must move away from this failed approach and support data minimization.

By the way, I don't think most people know how much data they are giving away. I just think 98 percent of the people -- and that may be generous -- don't. But I think we got -- the practice of only collecting, processing, and transferring data that is reasonably necessary, this is what I think we need to move to, and proportionate to provide or maintain a specific product or a service.

Mr. Britan, do you believe that all entities should be required to minimize the amount of data they collect on consumers by default?

*Mr. Britan. I do. I think data minimization is a good thing. It is not a new concept. It is something that existed since the Hew Report in 1973. I think data collection should be purposeful. Companies should know the purposes for which they are collecting data, and only collect the data that they believe they need to fulfill those purposes. This is -- this sort of proactive, planful approach to managing data will produce better privacy results.

*Mrs. Dingell. Consumers are deluged with constant breaches of their privacy and trust: weather apps collecting and selling users' location data to the highest bidder; data brokers selling -- and that is what -- this is what people don't realize is happening -- data brokers selling information collected from wellness apps about users' mental health conditions; and kids and teens' banking apps that collect sensitive data, name, birth dates, email addresses, GPS location history, purchase history, behavioral profiles, all about our nation's youth.

Mr. Britan, without data minimization requirements in place, are companies incentivized to collect, process, and transfer user data that is not necessary to provide a specific product's services?

And does over-collection of data increase the potential impact of a data breach?

*Mr. Britan. Absolutely. I think we need to shift the mindset of companies to, rather than thinking of data as an asset, to thinking of it as a potential liability. The more data you have, the more surface area you create for potential issues and -- such as improper access or misuse of that data. So even seemingly innocuous data can produce significant impacts if it is combined with other data sets or used in different contexts than what were contemplated.

So yes, we need data minimization, and the more data you have, the more chances you have of a breach.

*Mrs. Dingell. Thank you, and I yield back with an invitation to Detroit for next year.

*Mr. Bilirakis. Thank you very, very much. The gentlelady yields back, and I will recognize Mr. Armstrong for his five minutes of questioning.

*Mr. Armstrong. Thank you, Mr. Chairman.

Mr. Reed, COPPA imposes an actual knowledge standard on operators, meaning various duties are only imposed when an operator has information verifying that they are collecting or maintaining personal data on a minor.

ADPPA imposes a constructive knowledge standard on high-impact social media platforms that should have known the individual was a minor. Your testimony states that the constructive knowledge requirement may result in further data collection on all individuals, not just minors, in order to verify age. Can you explain that further?

*Mr. Reed. Sure. One of the problems that has existed from the initial step of COPPA was -- remember, COPPA's initial purpose was -- COPPA -- was to prevent advertising to children. COPPA is a collection standard, right? If you collect the information you need to first receive verifiable parental consent.

The problem when you start moving from an actual knowledge standard to a constructive knowledge standard is it essentially requires companies to start gathering more data on you to know whether or not -- what the condition of it is. And I said earlier in my testimony here, one of the problems is that we aren't empowering some of the platforms that might be able to send a signal or add a flag as a way for our developers to have that information before we ever collect something. Instead, it puts us on the mouse wheel of verifiable parental consent, which the parents don't like, which leads to problems.

So overall, though, we think that ADPPA -- can we say ADPPA now -- ADPPA moves us in the right direction. But that is the thing to make sure, that we are not actually burdening parents with more, not less.

*Mr. Armstrong. Do you think there is any interaction between that and the First Amendment right to anonymous free speech?

*Mr. Reed. Well, not -- we are focused here, instead of being on a constitutional law panel on apps. But absolutely, First Amendment is something that is critical to my members. They care about it. They talk about it. They send me emails about it. So absolutely, we need to make sure that whatever we are doing here around the privacy, that we do allow for anonymous speech in a manner that is -- since the birth of our nation and in the Federalist Papers.

*Mr. Armstrong. Your testimony also cautions against expanding the use of verifiable parental consent under COPPA, which you argue puts the onus on -- of privacy protections on the consumers. Can you explain those concerns?

*Mr. Reed. Yes, that is exactly what we were just saying, that VPC essentially requires the developer to affirmatively identify that it is the parent that is providing the permission to do things. Once you are through that gate, you can do a lot, and that has its own questions.

As I know Ms. Vance testified in her testimony, once you are through that COPPA verifiable parental consent gate, your access and ability to use the child's data raises its own questions. So I think VPC is onerous on the small businesses who impose it, although there are good companies like PRIVO and others that provide solutions. But it is also onerous -- it also creates uncertainty once you have gathered that data, especially if you have done it in a way that doesn't comport with PRIVO or other VPC safe harbors.

*Mr. Armstrong. Mr. Britan, this hearing is largely focused on sectoral privacy laws at the Federal level. But your testimony also states that Salesforce would welcome the passage of strong, comprehensive privacy laws at the state level. Does Salesforce support state privacy laws only in the absence of preemptive Federal comprehensive privacy law, or do you suggest that states should enact laws in addition to Federal privacy law?

*Mr. Britan. I think states should continue to be the laboratories for democracy, but I think we need a strong national standard. We need to speak with one voice as a country. And I think that the states have done great work, and we have supported that work because it has advanced the fundamental right to privacy in ways that didn't exist previously. But I think ADPPA is objectively the strongest privacy bill I have seen in the United States, and so I think it would set a strong national standard.

*Mr. Armstrong. But we also already exempted -- I mean, as part of ADPPA was, like, the Illinois Biometric Information Privacy Act. The case law that is produced from those laws is an important -- it has to be a risk for this community. And one of the -- to consider.

You know, an Illinois Supreme Court case that was decided months after we actually voted on ADPPA fundamentally altered the legal ramifications in Illinois and, by extension, the ADPPA. That court held that each scan or transmission of a biometric identifier or information constitutes a separate violation. So you are working at White Castle. You have to open a cash register with your fingerprint. You do it 10,000 times. That is 10,000 unique individual counts that can be brought against you.

So when we talk about national privacy, I mean, it just -- how does -- well, I will just ask you. How does Salesforce plan to mitigate for such compliance risks?

*Mr. Britan. These are tough issues.

I think, on the issue of preemption, Salesforce understands that we need a federal law. And we understand that preemption is one of the issues that is going to have to be a matter of compromise. And I think the compromise that was reached on ADPPA seemed reasonable. And if that is the compromise that has to be reached to get us a Federal law, that is -- then Salesforce would support that.

*Mr. Armstrong. And I think -- I mean, I can agree with that to some degree, except then you have a case that comes out exactly like this. And I just wonder how smaller businesses with less resources are going to be able to deal with it.

So I would love to, but I am out of time and they have called votes, so I will yield back.

*Mr. Bilirakis. The gentleman yields back. I know they called votes. We are going to try to get through this so that we won't have to come back, but we are going to do the best we can.

I will recognize Mr. Allen for his five minutes of questioning.

*Mr. Allen. Thank you, Chair Bilirakis, for convening this hearing, and I want to thank the witnesses for enduring this, and talking about this important issue. I would like to follow up on Chair Rodgers's -- the point she made in her questions about the dangers of tech companies recklessly testing their new AI models on the masses, specifically children.

Snapchat has a new feature called MyAI that integrates OpenAI's GPT technology into Snapchat's platform offering users which are on Snapchat, mainly teens, a new chat bot featured to interact with. This interaction can lead to hyper-specialized data sets on teens, including their thoughts, their questions, and their fears. Namely, anything a teen would think to ask chat bots. Snapchat would own this data, and plans to monetize it.

Mr. Britan, how should we think about data processing privacy in a world where users interact with chat bots on a wide array of topics?

*Mr. Britan. Yes, I think the best thing that we can do is pass comprehensive privacy law. I know I sound like a broken record.

*Mr. Allen. Yes.

*Mr. Britan. But I think these advancements hold great promise. There is also great potential pitfalls. And I think AI is powered by data, and the best thing we could do to ensure responsible AI and responsible chat bots is to pass comprehensive law regulating data broadly. That is missing in the U.S.

*Mr. Allen. Yes.

*Mr. Britan. And in the absence of that law in the U.S., the rest of the world is looking at this issue, and examining it, and pushing for responsible regulation. I think the U.S. has a very important voice in that conversation, and should be a part of that conversation, and can be if we pass ADPPA or a law like it.

*Mr. Allen. Right. Well, we keep harping on data minimization. And certainly, this is the opposite of data minimization.

You know, as a Member of Congress, I am concerned that we should be about -- I am concerned about what should be about AI-powered chat bots in the hands of our children. I have got 14 grandchildren, and I am worried about their interaction and the harm that this would do to their future. How valuable would this data set be to a business?

*Mr. Britan. It is hard for me to speak. I have worked at Salesforce, and I have worked at Microsoft to primarily B2B company Salesforce, entirely B2B. So I haven't had in-depth experience with understanding the value of children's data at Salesforce. We do have some educational projects, but we don't sell any of the children's data related to those products. So I am happy to say I haven't had to examine that issue in my career.

*Mr. Allen. And I assume you agree that this development makes a data privacy bill, which you said, even more timely.

And does everyone on this panel agree that this needs to be done as soon as possible?

*Mr. Britan. Yes. I am not in the business of working -- don't do children. I have three kids.

*Mr. Allen. Yes.

*Mr. Britan. I want them to be protected. We need a comprehensive privacy law to protect our kids.

*Mr. Allen. Good. With that, is there anything that you would like to add that might accelerate this process as far as the Congress is concerned?

*Mr. Reed. Congressman, I think the most important thing that would be helpful on this is reminding the Members of Congress that the small businesses in their district are actually part of this. And the better that you can do a preemptive privacy bill that helps the small businesses, it has as much of an impact.

I have heard a lot of discussion about Big Tech, but the people that rely on the technology are the people in the factories, in the companies. In your district there is Zapata Technologies that does some military contracts and other work. They depend on a robust data system and a robust privacy system. So if you are talking to your members on the floor and want to make the case, don't make the case about regulating Big Tech. It is for the benefit of their small businesses and U.S. innovation, so that we can compete on the global scale.

*Mr. Allen. Right. And I am in meetings, I am having meetings all week with small businesses from my district, and I am hearing the same thing.

So with that, I am out of time. Thank you so much for your time.

*Mr. Pence. [Presiding] The gentleman yields back. The chair now recognizes Congresswoman Harshbarger for five minutes.

*Mrs. Harshbarger. I will be as quick as I can. Thank you all for being here.

You know, I believe it is tremendously important that we establish a single national standard, really, before Chair Khan and her posse have the opportunity to go rogue and create more disastrous regulations, which they are prone to do.

And I want to focus on the idea of creating a private right of action as part of any legislation this committee is considering. And one consideration when we create a private right of action is running the risk of differing interpretations in different court districts, which results in more confusion of the rules, rather than more clarity.

So what can be done to mitigate some of these concerns with the private right of action so that our Federal standard brings real clarity to the regulated community?

And I guess I could start by asking you, Mr. Reed.

*Mr. Reed. Well, I think that we have all seen appropriate give-and-take on the question of private right of action. I think the main thing for small business is going to be not implementing a private right-of-action system that allows for what we call sue-and-settle, where you are going to send a letter to a small business, it is going to be for 50K. You talk to your attorney who is in your small town, they say, "I don't handle that stuff.'' And they say, "You know what, 50K? Just pay it.''

*Mrs. Harshbarger. Yes.

*Mr. Reed. So that is the part that we have to do. But I think the work, the bipartisan work that this committee has done to handle those questions, and hopefully some of their fellow members on the Senate side can get us through that hump by limiting it to a certain cadre of actions that can be taken.

*Mrs. Harshbarger. Yes, I have been a small business owner. And so, you know, and having pharmacies, that leads me right into my next question.

You know, I have had pharmacies, and what we do is we have to get licensed in several states. And listen, every state has different rules and regulations for my profession.

So I have learned that the most stringent regulation is the one we have to follow. It could be a Federal guideline from the FDA or it could be a state board guideline.

So if state data privacy standards are conflicting with the Federal standard, then companies may well have to listen to those, you know, stringent regulations. For example, you have talked about California, the blue state regulations, rather than the ones we set if there are conflicts. And so, you know, I don't want California telling me what I have to do in east Tennessee when it comes to how I practice pharmacy.

So how important is preemption in ensuring that we have clarity at a Federal level? And I go to you first, Mr. Reed.

*Mr. Reed. It is critical. And you raised an interesting point about levels. Some of the problems aren't levels, they are definitions. If one state says you call this data this, and this something else, or says --

*Mrs. Harshbarger. Yes.

*Mr. Reed. -- if you have a breach for a breach notification, you must immediately report. Others say you have to tell the police first. It isn't just that we have levels. I think too often when we discuss this issue, people say, well, one state can be a floor and another state -- and that doesn't create a ceiling. For small businesses, it might just be the definitions that are in that compliance regime that create the problem. It is not always about levels. So absolutely critical.

*Mrs. Harshbarger. Mr. Britan?

*Mr. Britan. Yes, we need to set a national standard for privacy. Privacy can't depend on zip code, and we can't have more powerful states dictating rights for other states.

I think preemption is going to require compromise. But I think, at the end of the day, it has -- it can't be a compromise that sets no level of preemption. It has to be a clear national standard that sets the rules of the road for the country.

*Mrs. Harshbarger. Yes. You know, if there are carve-outs to get this on the President's desk, my question is what provisions of the framework should we absolutely refuse to concede? Anybody?

[No response.]

*Mrs. Harshbarger. Or nobody.

*Mr. Reed. I think you have heard from everyone on the panel that data minimization is something that I don't think we can give up.

And I think that making sure that the exceptions -- that whatever you have to give up doesn't do some kind of odd carve-out that puts small businesses on an unbeneficial footing.

We want to -- we want privacy laws to apply to us. We want to abide -- because that creates trust, and that helps us get from small businesses to big businesses.

*Mrs. Harshbarger. It is almost like when you are audited by a PBM, and they ask for certain information. Don't give them any more than they ask for. It is just inviting more questions and more audits.

So with that, Mr. Chairman, I yield back.

*Mr. Pence. I thank the gentlelady. I now recognize myself for five minutes.

I would like to thank Chair Bilirakis and Ranking Member Schakowsky for holding this meeting, and all of you being here today at the end of the day.

You know, as the chairman already noted, this marks the thirty-sixth time Congress has had a hearing on the -- on privacy in the last five years. I heard that a couple of hearings ago, and I was just shocked. I couldn't believe it. And here, really, we are talking -- it is like a chipmunk in the wheel. We are just talking about the same thing over and over again, getting nothing done. And I don't think we are really getting the attention of Big Tech and those -- the violators in this environment.

You know, like many of my colleagues have discussed today, our increasingly digital world leaves Hoosiers and all Americans in the dark about who has access to their information. It is striking to me how little the consumers back home know about how much of their information is being collected, shared with third parties, and monetized without their informed consent. And that really bothers me. What am I getting for all the information you are taking from me all the time?

Just as truth in lending -- years ago I served on bank boards for many years -- was enacted to protect consumers from bad actors manipulating a complex financial industry, Congress needs to enact similar protections for all Americans where no current protections exist, like for Internet platforms that are becoming all but required to participate in modern society.

Unfortunately, this growth-at-any-cost mindset has led to more divisive interactions online and harmful rhetoric that is impacting social fabric.

There is nothing wrong with making money, but it seems to me that mass collection and sale of our information has become foundational to Big Tech's big business model, and now many other industries, as well.

Consumers deserve to have control over their information, how their information is collected, who has access to their data, the right to remove, private right of action, and where their data might be shared.

Mr. Britan, Axiom is commonly cited as one of the largest data brokers in the United States, collecting and selling information on hundreds of millions of Americans with whom they have no direct relationship. In the 12-month period preceding July 1st, 2022, Axiom reported receiving just 279 right-to-delete requests, despite at least 25 million American adults being eligible to make such a request under state laws.

One reason for this low participation rate could be that Axiom, like many of its peers, requires individuals to navigate a complex web portal in order to submit a relatively simple privacy request. It seems likely that data brokers have an incentive to make this process as difficult for individuals as possible. Even some of the non-Big Tech folks, it is difficult to get out of that.

Get -- the question. What is your opinion -- like -- the gentlelady asked this -- but the right-to-delete requests, especially for those directed at data brokers, what can we do about -- should we treat the data brokers differently than others?

*Mr. Britan. Absolutely, and I have supported a lot of the data broker legislation that we have seen across the country.

I think in order for the rights to be effective, people have to know who is processing their data so that they can make requests of those organizations. And I think that we need to make clear to people who has their data so that they can exercise their rights effectively.

I also think that we need to impose responsibilities on these companies that apply regardless of whether or not people take that action.

*Mr. Pence. Thank you.

Mr. Reed, though it was not mentioned today, we have discussed private right of action in past hearings. Without a well-defined private right of action in Federal law, how will consumers be able to actually enforce their right to delete and other important privacy rights?

I know you touched on that a moment ago, but what is the Federal way to do it?

*Mr. Reed. Well, I think right now, as you know, state AGs have power, and a bill like this would help them deal with it from a Federal -- from a national perspective.

I think that we -- the main caution that we would say -- and we have supported the work that you guys are doing on this legislation -- is to avoid making it so easy that we end up with a sue-and-settle system, which is hard on small business. But I think there are some ways to belts-and-suspenders this to put it into the hands of state AGs or other actions.

*Mr. Pence. Well, thank you for that. I hope we differentiate between the size of the folks involved.

And with that I yield back. I now recognize Mr. Obernolte for five minutes.

*Mr. Obernolte. [Presiding] Thank you. Well, thank you very much for the hearing, and thanks to all of you for being here.

Mr. Reed, I would like to start with a question for you. First of all, very -- I have a lot of respect for your organization. As an app developer myself, thank you for the good work that you do. You had some really interesting testimony about preemption and the need to take all of these disparate sectoral privacy standards and unify them under one universal rule at the Federal level. But I would like to ask kind of a follow-up question on preemption, because this is one of the big debates that we are having about the ADPPA here coming out of this committee, is the degree to which it should preempt state law.

So do you believe that we should fully preempt state law in the issue of digital data privacy, or do you believe that, as some states have requested that we do, that we merely establish a floor, and allow the individual states to go above that floor in their requirements on privacy if they wish to?

*Mr. Reed. I think we need fully -- a full Federal preemptive legislation. I think, without it, you cause international problems.

As I said earlier, tiny app developers will be in the international trade business. They will be selling their apps or making them available in 100 countries. So if the privacy laws aren't federally mandated across the board, then we have a problem even on international trade.

Secondarily, as you point out -- and I said this earlier -- there is this idea, or conflagration of this idea that it is levels. But sometimes it is just the definitions. So I might do the right thing, but I call it one thing in one state and one thing in another. And that means the compliance costs for a small business go up, because I have to create separate documents to talk about separate regimes with slightly different definitions. It is not always about levels. Sometimes it is just about what you call it.

*Mr. Obernolte. Yes, I completely agree with you. You know, I think sometimes we forget about the fact that when we allow this patchwork of regulation to exist with 50 different laws and 50 different states, it is very destructive to entrepreneurialism because the people that have the regulatory sophistication to deal with that are the big companies that have offices full of lawyers. And the people that don't have the sophistication to deal with that are two people in a garage that have to pay lawyers by the hour. So I am -- completely agree with you. I think that we have to be very careful about preemption. I think we need to decide what areas we are legislating in with our privacy bill, totally preempt within those areas, and then carve out the other areas to make it clear where states can act independently and where they can't.

And then, you know, just following up to that, I was in the California state legislature. I was one of the leads in drafting the California Consumer Privacy Act, and I think it is very important that we avoid some of the mistakes that were made with CCPA. We got a lot of things right. We were under time pressure -- without getting into detail -- to get that passed, but there were some kind of unexpected consequences that arose after that.

One of the main ones was that, much to our surprise, we thought this was going to be an iterative process, and once we passed it we knew we were going to have things that were missed as it was implemented, and we thought we were going to come along in subsequent years and fix it. You know, we would have a fix-up bill that -- the year after, another fix-up bill the year after that.

And what we had not anticipated is that when you create, even unintentionally, a regulatory landscape with winners and losers, all of the winners will then get together and try and prevent you from changing the rule the subsequent year, even if the rule was arbitrary, unintentional, or unfair. And that is just a fact of political life. And I had under-estimated how much that came to play.

So that is why it is so important that you are here, because I think stakeholder engagement is how you guard against that. And so I think we need to be very careful and deliberate about that.

Another thing that I think we need to be very careful about is that we are very specific in our choice of language in the bill. When you allow ambiguity to creep into what should be technical terms, particularly when it comes to things like data minimization, you need to be very careful that you are specific about what you mean when you say the data that you collect has to be necessary. Or if you say that it has to be related to the core business of your company, you better define what that means.

If you use a technical term, you better very carefully define it, because otherwise you will find yourself in the situation that we were in of having to watch a roomful of lawyers argue in front of a judge about what the intent of the author was, and that is something that, you know, when we abdicate our responsibility as legislators to the judicial branch, it serves no purpose.

So I am hoping that we can avoid some of that -- some of those complications this time around. And again, it is going to be through the engagement of stakeholders like the groups that you represent that we are able to get that done. So thank you very much for your testimony today, and we are looking forward to continuing to work with you to make sure we get this right.

So I will yield five minutes -- do we have anyone else up?

*Mr. Bilirakis. Do you want to close it?

*Mr. Obernolte. Sure.

*Mr. Bilirakis. Close it. But you don't get it next time.

[Laughter.]

*Mr. Obernolte. So I ask unanimous consent to insert in the record the documents included on the staff hearing documents list.

Without objection, that will be the order, and -- as there is no one here to object.

[The information follows:]

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

*Mr. Obernolte. I remind members they have 10 business days to submit questions for the record, and I ask the witnesses to respond to the questions promptly. I know you will.

Members should submit their questions by the close of business on May 11th.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 4:27 p.m., the subcommittee was adjourned.]